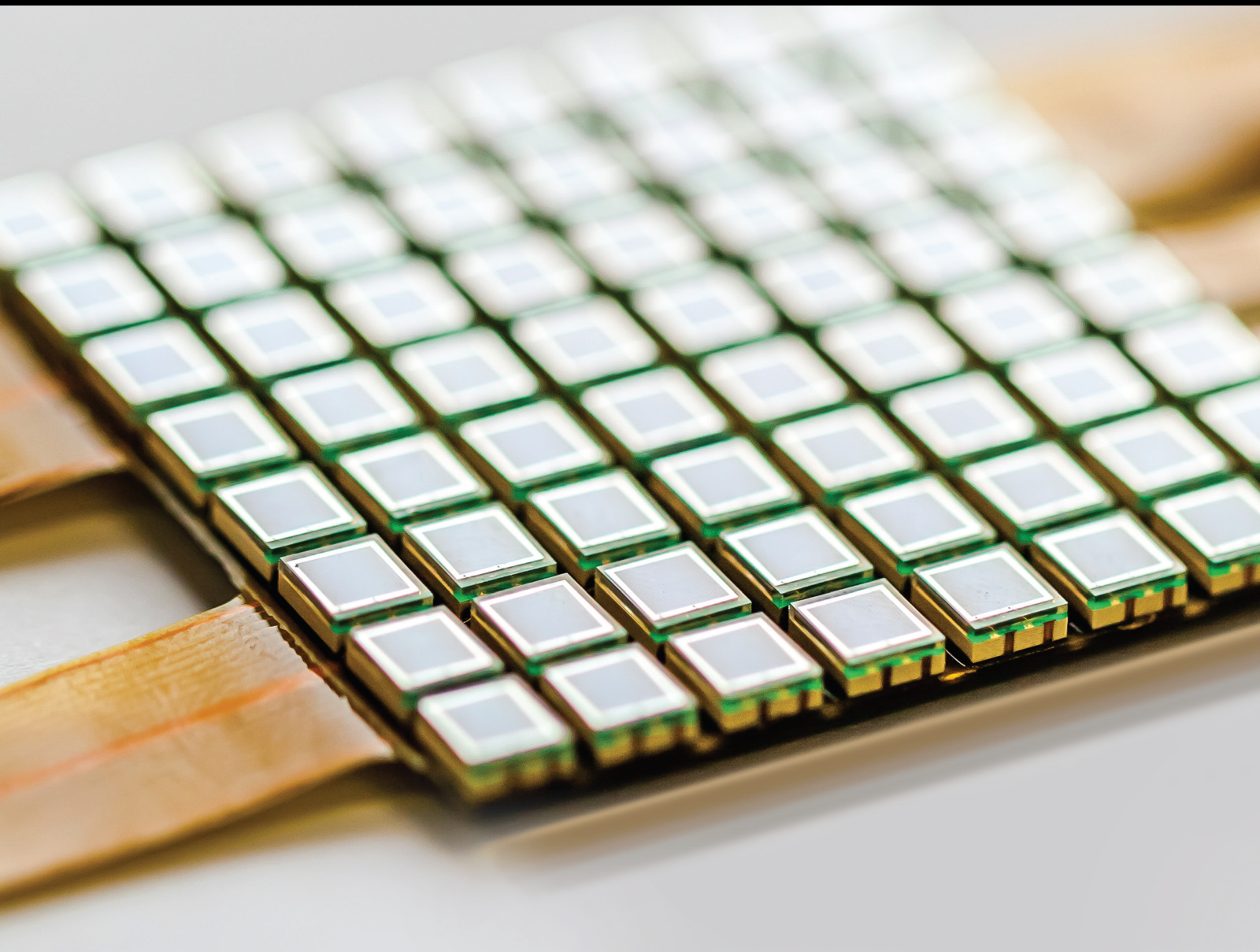


Recent Advances in Security and Privacy for Wireless Sensor Networks 2020

Lead Guest Editor: Fei Yu

Guest Editors: Chin-Chen Chang, Muhammad Khurram Khan, Iftikhar Ahmad, and Jun Zhang





**Recent Advances in Security and Privacy for
Wireless Sensor Networks 2020**

**Recent Advances in Security and Privacy
for Wireless Sensor Networks 2020**

Lead Guest Editor: Fei Yu

Guest Editors: Chin-Chen Chang, Muhammad
Khurram Khan, Iftikhar Ahmad, and Jun Zhang






Copyright © 2021 Hindawi Limited. All rights reserved.

This is a special issue published in "Journal of Sensors." All articles are open access articles distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Chief Editor

Harith Ahmad , Malaysia

Associate Editors

Duo Lin , China
Fanli Meng , China
Pietro Siciliano , Italy
Guiyun Tian, United Kingdom

Academic Editors

Ghufran Ahmed , Pakistan
Constantin Apetrei, Romania
Shonak Bansal , India
Fernando Benito-Lopez , Spain
Romeo Bernini , Italy
Shekhar Bhansali, USA
Matthew Brodie, Australia
Ravikumar CV, India
Belén Calvo, Spain
Stefania Campopiano , Italy
Binghua Cao , China
Domenico Caputo, Italy
Sara Casciati, Italy
Gabriele Cazzulani , Italy
Chi Chiu Chan, Singapore
Sushank Chaudhary , Thailand
Edmon Chehura , United Kingdom
Marvin H Cheng , USA
Lei Chu , USA
Mario Collotta , Italy
Marco Consales , Italy
Jesus Corres , Spain
Andrea Cusano, Italy
Egidio De Benedetto , Italy
Luca De Stefano , Italy
Manel Del Valle , Spain
Franz L. Dickert, Austria
Giovanni Diraco, Italy
Maria de Fátima Domingues , Portugal
Nicola Donato , Italy
Sheng Du , China
Amir Elzwawy, Egypt
Mauro Epifani , Italy
Congbin Fan , China
Lihang Feng, China
Vittorio Ferrari , Italy
Luca Francioso, Italy



Libo Gao , China
Carmine Granata , Italy
Pramod Kumar Gupta , USA
Mohammad Haider , USA
Agustin Herrera-May , Mexico
María del Carmen Horrillo, Spain
Evangelos Hristoforou , Greece
Grazia Iadarola , Italy
Syed K. Islam , USA
Stephen James , United Kingdom
Sana Ullah Jan, United Kingdom
Bruno C. Janegitz , Brazil
Hai-Feng Ji , USA
Shouyong Jiang, United Kingdom
Roshan Prakash Joseph, USA
Niravkumar Joshi, USA
Rajesh Kaluri , India
Sang Sub Kim , Republic of Korea
Dr. Rajkishor Kumar, India
Rahul Kumar , India
Nageswara Lalam , USA
Antonio Lazaro , Spain
Chengkuo Lee , Singapore
Chenzong Li , USA
Zhi Lian , Australia
Rosalba Liguori , Italy
Sangsoon Lim , Republic of Korea
Huan Liu , China
Jin Liu , China
Eduard Llobet , Spain
Jaime Lloret , Spain
Mohamed Louzazni, Morocco
Jesús Lozano , Spain
Oleg Lupan , Moldova
Leandro Maio , Italy
Pawel Malinowski , Poland
Carlos Marques , Portugal
Eugenio Martinelli , Italy
Antonio Martinez-Olmos , Spain
Giuseppe Maruccio , Italy
Yasuko Y. Maruo, Japan
Zahid Mehmood , Pakistan
Carlos Michel , Mexico
Stephen. J. Mihailov , Canada
Bikash Nakarmi, China

Ehsan Namaziandost , Iran
Heinz C. Neitzert , Italy
Sing Kiong Nguang , New Zealand
Calogero M. Oddo , Italy
Tinghui Ouyang, Japan
SANDEEP KUMAR PALANISWAMY ,
India
Alberto J. Palma , Spain
Davide Palumbo , Italy
Abinash Panda , India
Roberto Paolesse , Italy
Akhilesh Pathak , Thailand
Giovanni Pau , Italy
Giorgio Pennazza , Italy
Michele Penza , Italy
Sivakumar Poruran, India
Stelios Potirakis , Greece
Biswajeet Pradhan , Malaysia
Giuseppe Quero , Italy
Linesh Raja , India
Maheswar Rajagopal , India
Valerie Renaudin , France
Armando Ricciardi , Italy
Christos Riziotis , Greece
Ruthber Rodriguez Serrezuela , Colombia
Maria Luz Rodriguez-Mendez , Spain
Jerome Rossignol , France
Maheswaran S, India
Ylias Sabri , Australia
Sourabh Sahu , India
José P. Santos , Spain
Sina Sareh, United Kingdom
Isabel Sayago , Spain
Andreas Schütze , Germany
Praveen K. Sekhar , USA
Sandra Sendra, Spain
Sandeep Sharma, India
Sunil Kumar Singh Singh , India
Yadvendra Singh , USA
Afaque Manzoor Soomro , Pakistan
Vincenzo Spagnolo, Italy
Kathiravan Srinivasan , India
Sachin K. Srivastava , India
Stefano Stassi , Italy

Danfeng Sun, China
Ashok Sundramoorthy, India
Salvatore Surdo , Italy
Roshan Thotagamuge , Sri Lanka
Guiyun Tian , United Kingdom
Sri Ramulu Torati , USA
Abdellah Touhafi , Belgium
Hoang Vinh Tran , Vietnam
Aitor Urrutia , Spain
Hana Vaisocherova - Lislalova , Czech
Republic
Everardo Vargas-Rodriguez , Mexico
Xavier Vilanova , Spain
Stanislav Vitek , Czech Republic
Luca Vollero , Italy
Tomasz Wandowski , Poland
Bohui Wang, China
Qihao Weng, USA
Penghai Wu , China
Qiang Wu, United Kingdom
Yuedong Xie , China
Chen Yang , China
Jiachen Yang , China
Nitesh Yelve , India
Aijun Yin, China
Chouki Zerrouki , France

Contents

An Incentive and Reputation Mechanism Based on Blockchain for Crowd Sensing Network

Zainib Noshad, Asad Ullah Khan, Shahid Abbas, Zain Abubaker, Nadeem Javaid , Muhammad Shafiq, and Jin-Ghoo Choi 

Research Article (14 pages), Article ID 1798256, Volume 2021 (2021)

Power Grid-Oriented Cascading Failure Vulnerability Identifying Method Based on Wireless Sensors

Shudong Li , Yanshan Chen, Xiaobo Wu , Xiaochun Cheng , and Zhihong Tian 

Research Article (12 pages), Article ID 8820413, Volume 2021 (2021)

Research on the Evaluation Model for Wireless Sensor Network Performance Based on Mixed Multiattribute Decision-Making

Jiekun Song , Yemeng Zhang , Zhihao Zhao , and Rui Chen 




Research Article (13 pages), Article ID 8885009, Volume 2021 (2021)

A Compact FPGA-Based Accelerator for Curve-Based Cryptography in Wireless Sensor Networks

Miguel Morales-Sandoval , Luis Armando Rodriguez Flores, Rene Cumplido, Jose Juan Garcia-Hernandez, Claudia Feregrino, and Ignacio Algreto



Research Article (13 pages), Article ID 8860413, Volume 2021 (2021)

On the Exploitation of Blockchain for Distributed File Storage

Zuoting Ning, Lijun Xiao , Wei Liang , Weiqi Shi, and Kuan-Ching Li 



Research Article (11 pages), Article ID 8861688, Volume 2020 (2020)

An Identity-Based Anonymous Three-Party Authenticated Protocol for IoT Infrastructure

Akasha Shafiq, Muhammad Faizan Ayub, Khalid Mahmood , Mazhar Sadiq, Saru Kumari, and Chien-Ming Chen 


Research Article (17 pages), Article ID 8829319, Volume 2020 (2020)

Offline/Online Outsourced Attribute-Based Encryption with Partial Policy Hidden for the Internet of Things

Xixi Yan, Guanghui He , Jinxia Yu, Yongli Tang , and Mingjie Zhao


Research Article (11 pages), Article ID 8861114, Volume 2020 (2020)

Reversible Data Hiding for Encrypted 3D Model Based on Prediction Error Expansion

Li Li, Shengxian Wang, Ting Luo , Ching-Chun Chang, Qili Zhou, and Hui Li

Research Article (14 pages), Article ID 8851999, Volume 2020 (2020)

Construction of a Security Vulnerability Identification System Based on Machine Learning

Kebin Shi, Yonghui Dai , and Jing Xu

Research Article (9 pages), Article ID 7358692, Volume 2020 (2020)

Research Article

An Incentive and Reputation Mechanism Based on Blockchain for Crowd Sensing Network

Zainib Noshad,¹ Asad Ullah Khan,¹ Shahid Abbas,¹ Zain Abubaker,¹ Nadeem Javaid ¹,
Muhammad Shafiq,² and Jin-Ghoo Choi ²

¹Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan

²Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

Correspondence should be addressed to Nadeem Javaid; nadeemjavaidqau@gmail.com and Jin-Ghoo Choi; jchoi@yu.ac.kr

Received 8 February 2020; Accepted 19 June 2021; Published 9 July 2021

Academic Editor: Qiang Wu

Copyright © 2021 Zainib Noshad et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Nowadays, sensors inserted in mobile applications are used for gathering data for an explicit assignment that can effectively save cost and time in crowd sensing networks (CSNs). The true value and essence of gathered statistics depend on the participation level from all the members of a CSN, i.e., service providers, data collectors, and service consumers. In comparison with the centralized conventional mechanisms that are susceptible to privacy invasion, attacks, and manipulation, this article proposes a decentralized incentive and reputation mechanism for CSN. The monetary rewards are used to motivate the data collectors and to encourage the participants to take part in the network activities. Whereas the issue of privacy leakage is dealt with using Advanced Encryption Standard (AES128) technique. Additionally, a reputation system is implemented to tackle issues like data integrity, fake reviews, and conflicts among entities. Through registering reviews, the system encourages data utilization by providing correct, consistent, and reliable data. Furthermore, simulations are performed for analyzing the gas consumed by smart contracts. Similarly, the encryption technique is ratified by comparing its execution time with other techniques that are previously used in literature. Lastly, the reputation system is inspected through analyzing the gas consumption and mining time of input string length.

1. Introduction

The rapid expansion and revolutionary developments in technology, such as smartwatches, smart glasses, wearable devices, and smartphones that have embedded sensors, provide data collection opportunities to organizations. These opportunities give access to multiple organizations and companies to raw data that can be sensed from a particular environment. This forthcoming process is the new direction in the market [1]. The progression in the technology has given access to so many applications to gather data through the mobile crowd sensing network (MCSN). This mechanism operates by contracting out the sensing task to a voluntary crowd known as workers or data collectors [2]. The key objective of these workers is to finish their designated tasks for which they are compensated through a variety of incentives. The type of incentive depends on the service provider also known as task requester. The inspiration for this approach

is taken from a conventional process known as a win-win situation. Here, all the parties involved, i.e., server and a client, are provided a chance to cooperate and work together with each other for cultivating a mutually beneficial resolution.

The smart contracts are incorporated as a secure transmission medium by imposing the defined criteria autonomously. The purpose of incorporating the reputation system in the proposed scenario is to preserve the integrity and reliability of data for promoting trust among the service consumers. The acronyms are listed in Table 1.

From a commercial perspective, many scholars have explored this new trend to attain maximum advantage from crowd sensing network (CSN). Thus, a service-based approach is another point of view that has been researched by authors [3]. Furthermore, a new entity [4], i.e., the service consumer is led in this picture for gaining profit by the sensed data acquired by workers. Otherwise, if the third entity is not considered, the massive amount of data collected goes into

TABLE 1: List of acronyms.

Acronyms	Full form
AES	Advanced encryption standard
CSN	Crowd sensing network
DES	Data encryption standard
DTRPP	Dynamic trust relationships aware data privacy protection
GPS	Global positioning system
IoT	Internet of things
MCSN	Mobile crowd sensing network
MT	Merkle tree
QUOIN	Quality and usability of information
RAF	Review automatic filtering
RSA	Rivest-Shamir-Adleman

waste. Additionally, the significant time spent, efforts, and resources on this procedure also go in vain. To improve, achieve organizational goals, and drive towards success, it is a necessity for businesses to process and analyze the data [5]. Therefore, the raw data acquired by the data collectors are sold that can help out organizations to fill up the loopholes and produce radical and dynamic leads for projects.

The multifarious issues have become apparent with the CSN based platforms, which have provided an effective mechanism for sensing data at a cheaper rate with many advantages. Numerous researchers have indicated that CSN has become a constructive tool for obtaining quality data, which was previously difficult to obtain [4]. An incentive mechanism has been devised, which compensates the workers for spending their resources and collaterals. Moreover, CSN platforms' strength is ensuring trustworthiness in their efficient requisite services. For optimum service utilization, the customer of such a facility must know the kind of data he wants to acquire, and then the transaction should be made. Furthermore, CSN is branched into two more domains, i.e., in-volunteer (opportunistic) and volunteer (participatory) [6–8]. Such category arrangements assist beneficiaries in their decision for resource allocation, tasks, and resources to be utilized.

Several incentives have been devised, including socially aware incentive mechanisms for the MCSN [9] to resolve issues faced by CSN, like quality and information usability (QUOIN) [10], and numerous compensation (monetary) approaches. A central authority is established for these mechanisms [11]; thus, a single point of failure may occur. Moreover, the participation of malicious users can expose these systems to Sybil and Distributed Denial of Service (DDoS) attacks. The blockchain has shown its tendency to be the best claim for centrist approaches of the CSN technology. Figure 1 is taken from [11]. Blockchain has also a lot of applications in energy trading in smart grids, like [12–14], in food supply management, like [15], and in data sharing, like [16].

In this article, we have proposed a decentralized incentive and reputation mechanism for CSN with two communication paradigms. The system is further divided based on these two paradigms, i.e., incentive mechanism between service

providers and data collectors, and a reputation system between service providers and consumers. Further, the Advanced Encryption Standard (AES128) is also implemented for retaining the privacy of data collectors.

1.1. Contributions. This work is an extension of [17]. The contributions of this paper are summarized as follows.

- (i) A blockchain-based incentive and reputation mechanism is proposed for CSN
- (ii) To ensure data quality, a rating mechanism is implemented where requesters rate the acquired data from service providers
- (iii) The issue of privacy of data collectors is tackled using the AES128 encryption technique
- (iv) Furthermore, the performance of the proposed system is evaluated by three widely used performance measures for blockchain, which are stated below
 - (a) Gas consumption of incentive smart contracts
 - (b) Mining time against different string input lengths of the reputation system
 - (c) Gas consumption against different input string values of the reputation system
 - (d) The comparison of execution time between different cryptographic techniques

1.2. Organization. The paper is further organized as follows. Section 2 provides the literature review, which is further divided into three categories, i.e., blockchain-based CSN, incentive mechanism-based CSN, and privacy mechanism-based CSN. Section 3 describes the motivation behind the proposed system and the identified problem. Section 4 presents the explanation of the proposed system model. In Section 5, an analysis of security, privacy, and robustness is discussed and Section 6 presents the details of experimental results, whereas the paper is concluded in Section 7.

2. Related Work

The related work for CSN is divided into three categories: blockchain, incentive, and privacy mechanisms.

2.1. Blockchain-Based CSN. CSNs are categorized as generally large groups of people that possess mobile devices for different purposes. These devices can sense and process the shared data that can be utilized to measure, map, analyze, and extract important information. Most smart mobile devices, e.g., phones and tablets can sense several inputs, such as ambient light, location, noise, and movement. In [18], a blockchain-based incentive system for CSN is proposed. It works on the principle of motivating the participants through retaining their privacy. Mainly, the system takes into account the truthfulness by introducing a cryptocurrency token as a premium to the participants. With this system, high-quality users get a reward and it is stored in the blockchain. The

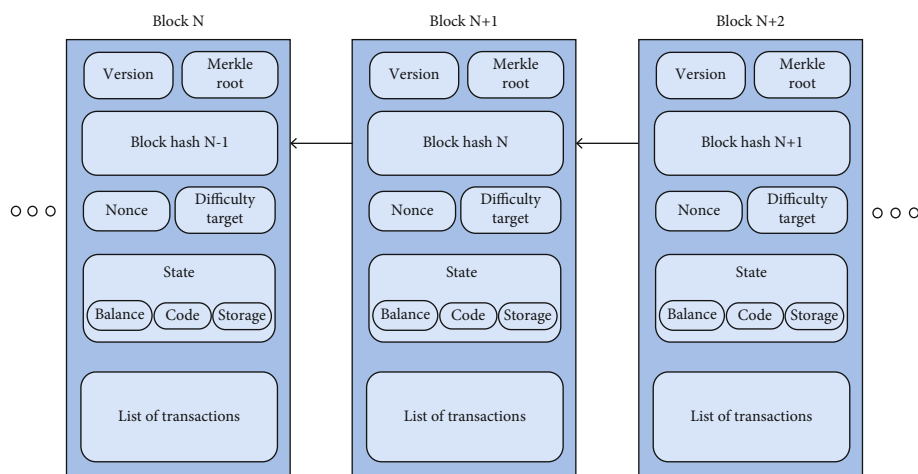


FIGURE 1: Blockchain structure.

process integrates a server that publishes a sensing task, users who complete and upload a task assignment, and the miners that verify the quality of data. Once the verification is done, the transactions must be validated, and the rewards are distributed by the server to the participants. While in [19], the authors propose a blockchain-based mechanism that uses location privacy preservation as an incentive in CSNs. The mechanism emphasizes to protect any information and provides rewards to participants that increase the users' participation. The experimental tests were conducted with a total of 10 participants in a campus environment, and the obtained results are effective in encouraging the participation of users. In [20], the authors have introduced a crowdsensing blockchain-based system where both the miners and workers that are involved in sensing task are rewarded via a predefined incentive system, which incorporates authentic anonymity and robustness. The related work is summarized in Table 2.

2.2. Incentive Mechanism-Based CSN. The system proposed in [10] is known as QUOIN. It ensures the usability and quality of the information for CSN applications. The theory of the Stackelberg game is implemented so that every participant is benefited by an equal and sufficient part of incentives. This system is evaluated by conducting a case study. The obtained results show the efficacy of the system for motivating the workers to participate.

The authors of [21] have proposed a monetary encouragement mechanism for CSN. The system is based on contract theory. The process includes a trust plan implemented between the platform and mobile network users. The trust scheme includes direct and indirect trust patterns. A contract is established that has incentive allotment criteria outline. Along with the platform's profitability, this contract appeases the customer's incentive agreeableness. Furthermore, in [9], the authors have suggested a new scheme that is called social incentive mechanism. As the name suggests, it is based on providing incentives to the friends of the participants in the network. It intensifies the social bonds among network users, which in turn pro-

motes global ties. The incitement helps to promote participation as when a user motivates its friends to participate, it is rewarded with an increased payback. The networks based on the interdependent relationship are highly benefited from this kind of incentive approach.

The authors in [22] have presented a case study with the ParticipAct platform and living lab. The experiment is conducted at a University located in Bologna. The experiment involves a total of 170 students, and the duration of the experiment is 365 days. The crowd users participated in several crowdsensing tasks and campaigns. Moreover, mobile phones were accessed passively, and the user's active cooperation and collaboration are provoked. The article outlines the platform's architecture, design, features, and reports with integral results.

2.3. Privacy Mechanism-Based CSN. The encryption techniques play a vital role in preserving the privacy of any participant. The process of encryption and decryption is compared by the authors of [26, 27] such as Rivest-Shamir-Adleman (RSA), AES, Blowfish, and Data Encryption Standard (DES). The features considered for comparing the techniques are time, avalanche effect, entropy, and memory used. Similarly, in [23], the authors proposed a platform where CSN is promoted as a contribution. Nonetheless, whenever there are people entangled, there is a possibility of exploitation of privacy. For CSN, privacy leakage is a loose end because this platform purely relies on participant's in-volunteering or volunteering actions. This kind of problem is tackled using AES256 for preventing the exploitation of the user's privacy. Likewise, in [19], affine cipher is implemented for a similar issue as mentioned above.

Additionally, for conventional CSNs [24], Dynamic Trust Relationships Aware Data Privacy Protection (DTRPP) mechanism is used for preserving the confidentiality of the participants. The platform integrates the trust management mechanism with the public key. The results display the improved performance of the system in terms of delivery, load rate, and average delay as compared to traditional mechanisms. Similarly, in [25], the authors have suggested a

TABLE 2: Summary of related work.

Schemes	Contributions	Limitations
Blockchain-based CSN		
Blockchain-based incentive mechanism for CSNs [18]	Ensures data quality, increases participation level, and preserves the privacy of the workers	Collusion attacks are ignored between anonymity groups and miners
A decentralized privacy-preserving incitement mechanism for CSNs [19]	Ensures privacy by using affine cipher and stimulates user involvement	Insecure communication platform and does not consider service consumers
Blockchain-based crowd sensing system (BCS) [20]	Provides authentic anonymity of the workers and system robustness	Possibility of privacy leakage of workers while submitting location for efficient job allocation
Incentive mechanism-based CSN		
A social incentive mechanism for CSN [9]	Promotes global cooperation	Structure of participant's social relationship is not considered
Incentive mechanism for CSN named as QUOIN [10]	Provides quality and usability of information and stimulates participation rate	Single point of failure and mutability
Incentive mechanism based on contract theory for mobile CSNs [21]	Increases participation rate and maximizes platform's profitability	Centralized server causes delay in performance
Incentive mechanism involving ParticipAct platform for CSNs [22]	Promotes user active collaboration	Single point of failure and no transparency
Privacy mechanism-based CSN		
CSN as a service and contribution [23]	Preserved privacy with AES256	No traceability mechanism
DTRPP [24]	Combined public key with trust management mechanism for tackling the issue of privacy	Ineffective in terms of cost
Location preserving mechanism of mobile users by combining k -anonymity and differential privacy [25]	Protects location of mobile users	Ineffective in terms of cost

system to shield and safeguard the location of the users participating in the network by integrating differential privacy-preserving and k -anonymity.

3. Motivation and Problem Statement

In this section, the motivation behind the proposed system is discussed along with the problem statement.

3.1. Motivation. In [20], the authors have proposed a quality-driven auction-based incentive mechanism for MCSN. Similarly, in [28], the authors have introduced TaskMe. It is also based on a cross-community and quality-enhanced incentive mechanism for MCSNs. These incentive-based mechanisms motivate the participants to take part in the task sensing and consequently enhance the quality of data. The higher quality of data provided by users, the more reward a server returns to users. In [4], a Stackelberg game theory model-based incentive mechanism for CSN is proposed where the authors have considered three entities instead of two, i.e., service providers, service consumers, and data collectors. Furthermore, in order to recruit mobile workers, the authors of [7] have proposed reputation-aware recruitment and credible reporting for platform utility in MCSN. The mechanism is aimed at hiring mobile workers based on the reputation for quality reporting with the intention of platform profit maximization for an Internet of Things (IoT's) scenario. By taking

the motivation from the above work, in this paper, we have proposed a blockchain-based decentralized system with seven groups having distinct roles, i.e., service providers, service consumers, data collectors, blockchain, communication platform, arbitrator, and a reputation system for ensuring the integrity and immutability of data through registered reviews.

3.2. Problem Identification. In [19], a decentralized virtual credit incentive mechanism is proposed while providing privacy protection for CSN entities. The main objective is to tackle two problems, i.e., stimulating user participation and privacy exposure. Affine cipher is used for privacy protection, and the other issue is tackled by giving the guarantee of preserving the participant's privacy. However, it is affiliated with the class of classical monoalphabetic substitution schemes. It is also liable to all the cipher attacks. Furthermore, the medium used for communication is not a smart contract, and the technique used for encryption is implemented separately. Also, the third entity used for utilizing the data, i.e., service consumers is not considered in the proposed system.

Moreover, to build trust between the service providers and consumers, it is necessary to build a system, which assures the integrity and reliability of data being sold out to consumers. To tackle such a challenge, a reputation system is introduced for the proposed scenario and the motivation is taken from [7, 29]. Another issue is raised during the

system development, i.e., no stimulus is provided for the consumers to register a review. There is no incentive for consumers for contributing their time and computational resources for registering a review. This problem can damage the system's performance.

To confront the aforementioned limitations, we have recommended a scenario, which is then divided into two units of communication that are explained below.

3.2.1. Communication between Data Collectors and Service Providers. In the suggested scenario, the service provider establishes a smart contract. AES128 encryption technique is applied to guarantee that workers' identities are preserved while surrendering their location for task assignment; hence, guaranteeing the privacy of data collectors. Furthermore, incentives are allotted to all the data collectors immediately to motivate user participation.

3.2.2. Communication between Service Consumers and Service Providers. To initiate communication between a consumer and service provider, a smart contract is deployed that triggers the function of the service request and its response, accordingly. Further, to check the integrity of data, a decentralized reputation mechanism is implemented between them. To solve the problem of motivating consumers for registering a review, an incentive mechanism is also introduced for service consumers. The reward is issued only to those consumers, who wish to register their reviews and contribute to enhancing the performance of the whole blockchain-based reputation mechanism for CSN. Furthermore, a fake review is another major challenge in the reputation system. To eliminate the fake reviews, which could be done by any consumer or an opponent company/organization, the Revain platform is used to make sure that the module identifies fake reviews. Moreover, in case of a dispute between a service consumer and a provider, the arbitrator steps in to resolve the clash and restores all the collaterals. The proposed system is compared with the existing systems in Table 3.

4. System Model

The system model of the proposed mechanism is further divided into two modules, i.e., incentive system and reputation system. They are elaborated in the subsections below.

4.1. Incentive System. This system is developed for providing an incentive mechanism based on blockchain for CSN. Four entities are participating in the proposed scenario, i.e., service provider, arbitrator, service consumers, and data collectors. The following words, i.e., requester and service provider, data collector, and worker are being used alternatively throughout the paper. The aspects of each role are defined in Table 4.

The smart contract is initially called by a requester, and it sets the demands of the data sensing task. Service providers deposit some amount that is later established as a monetary reward for the workers. The task assignment is finally authorized and broadcasted in the network. To preserve the privacy of the workers for promoting and motivating their participation in tasks, AES128 is used to encrypt private information, therefore, preventing the exploitation of pri-

vacancy. Thereafter, when the data collectors submit their assigned task is verified by the miners. After verification, the rewards are immediately allotted that are set aside in the smart contract's protocol. The prompt incentives build up the repute of the system. Also, it encourages both miners and data collectors for their devotion. Similarly, trust is already established between service providers and other participants because of the rules set in the smart contract. As a result, a requester is considered a reliable entity. Additionally, data collectors are charged with a definite aggregate of gas while posting the sensed data. The cumulative gas serves as a security deposit by the data collectors and guarantees the authenticity of the participant. This process aids in avoiding various kinds of attacks. The motivation for the proposed system model is taken from [19, 29, 30], as shown in Figure 2. The interaction between service consumers and provider takes place through a separate smart contract as shown in Figure 2. If a consumer requires service from a requester, it inquires for a review before sending the request. This mechanism is shown in Figure 3. A specific request is sent by the consumer for establishing a smart contract to the requester. The payment is made immediately in exchange of the requested data. Also, the usage of smart contracts aids in getting the job done efficiently and effectively. Additionally, it also dismisses the possibility of any blunder that may occur in traditional agreements or contracts.

4.2. Reputation System. Figure 3 is the proposed system model, which is deployed between service consumers and service provider. The purpose of this mechanism is to make sure that the service consumer knows the reputation of data from the previous reviews before purchasing. The smart contract used for this review system uses four functions, and each of them performs operations to check the existence, registration, and content of a review or the ratings associated with it. The details of these functions are described below.

- (i) *IsReviewExist()*. This function is used to send a request for displaying the existing reviews of the data requested by the service consumer
- (ii) *GetReview()*. This function is used to fetch the requested reviews, if they exist; otherwise, the value count comes as zero
- (iii) *GetRating()*. This function is used to fetch the rating of the data
- (iv) *SetReview()*. This function is used for registering a review after purchasing data in order to show its authenticity and usability to other service consumers

The comparison between existing centralized and decentralized reputation system is taken from [29] as shown in Table 5.

4.2.1. Fake Reviews. In order to tackle the issue of review manipulation [31], which could be done by any consumer or an opponent company/organization, we have used the Revain platform [32] to filter out fake reviews. The steps of this system are stated below.

TABLE 3: Comparison with existing work.

References	Smart contracts	Service consumers	Encryption	Reputation system	Identification of fake reviews	Dispute resolution
Reputation aware recruitment platform for CSN [7]		✓		✓		
Blockchain-based incentive mechanism for CSN [19]			✓			
Smart contract-based review system [29]	✓	✓		✓		
Proposed mechanism: blockchain-based incentive and reputation mechanism	✓	✓	✓	✓	✓	✓

TABLE 4: Roles of entities of a CSN.

Participants	Roles
Requester/service provider	Publishes an assignment in the network and accommodates services for consumers
Service consumers	Request and inquire data. Then, utilize the data obtained by a data collector
Worker/data collectors	Measures the necessary data of interest in accordance with the defined criteria using smart gadgets
Arbitrator	It is a trusted entity by the requester, consumers, and workers. The role of the arbitrator is to resolve disputes between the requester and the consumer. It also settles the quarrel by downloading the same item requested by the consumer and decides whether the complaint filed is valid or not.

- (i) *Review Automatic Filtering (RAF)*. When the user submits a review, it undergoes automatic moderation via machine learning and neural networks. This determines the emotional content of the review like consumer experience with the product. This filtering process module is used to provide an authentic review
- (ii) *Storage*. Following RAF filtering, the review is saved on the Ethereum blockchain to prevent its editing. The data is stored in blockchain via smart contracts
- (iii) *Verification*. To verify the consistency of review, a Merkle tree (MT) hash algorithm is used. In MT, a group of hashes are hashed together to create hash of hashes in order to create a root hash at the final step. To figure out whether something has changed anywhere in the posted review or not, we only check the root hash mutability. If there is a change at root hash, then, the tree is followed down to inspect where the change is made
- (iv) *Incentives*. To assure proper usage of the platform, this mechanism encourages the users by providing incentives. Users who give exponentially good reviews have a chance of earning more rewards

4.2.2. *Unsuccessful Download or Dispute Settlement*. To resolve the conflict between customer and service provider, an arbitrator steps in. The procedure followed by this module is as follows.

- (i) The customer files a complaint regarding unsatisfactory results

- (ii) The arbitrator gains access of the customer's token and downloads the same content
- (iii) If the content is downloaded and the result is positive, the customer's claim is falsified and the service provider is paid according to the settled agreement in the smart contract. Otherwise, the collaterals are refunded and returned to the customer

5. Security, Privacy, and Robustness Analysis

In this section, the proposed mechanism is critically analyzed based on three inherent blockchain features, i.e., security, privacy, and robustness. It is further elaborated in the subsections below.

5.1. *Security Analysis*. In traditional CSN, a worker's privacy is disclosed during the payment process. To avoid such security threats, third parties are involved to guarantee a proper and safe payment of transactions. However, it is difficult to trust a third party for providing a secure environment. To prevent this kind of situation in the proposed mechanism, we take advantage of the inherent blockchain properties.

There is no third-party involvement while a worker and a requester sign a smart contract on the blockchain. The rules and regulations of payment, reward, and evaluation criteria of the sensory data are already present in the smart contract. Once the smart contract is deployed and triggered, the predefined functions are executed automatically, and consequently, the rewards are paid.

In this paper, the proof of work consensus mechanism is used by miners to add a new block in the blockchain. In this mining algorithm, each miner node validates the transactions independently. When a node generates a new block, it

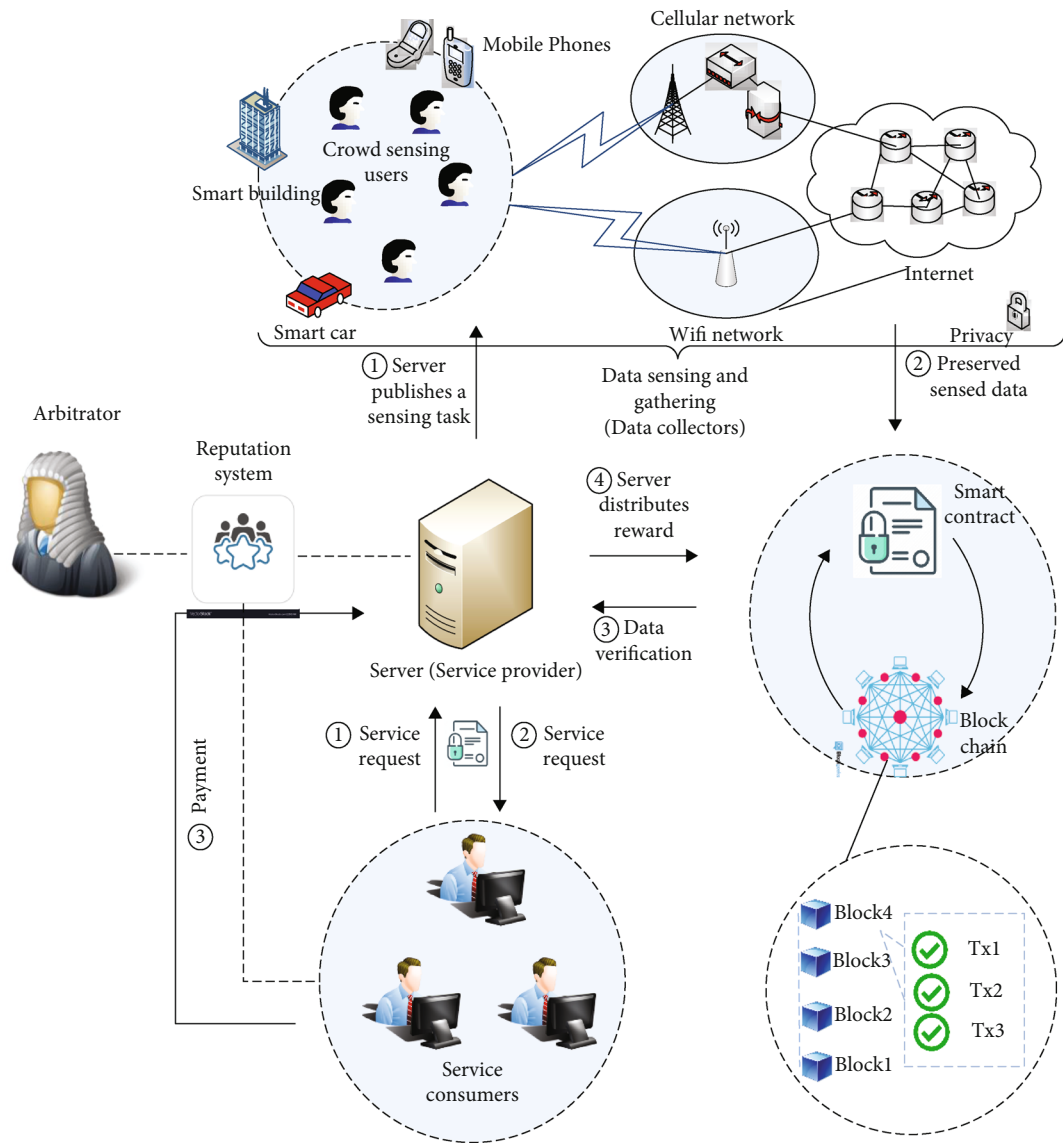


FIGURE 2: Blockchain-based incentive and reputation mechanism for CSNs.

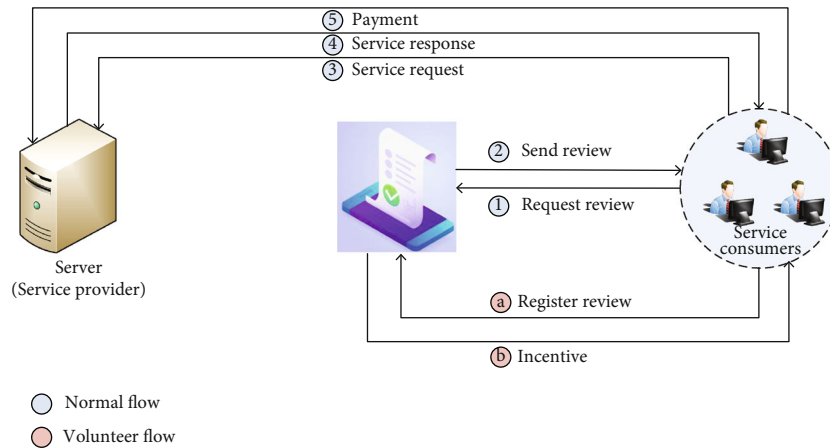


FIGURE 3: Reputation system for CSN.

TABLE 5: Comparison of centralized with decentralized model of reputation system.

Parameters	Server-client reputation system	Blockchain-based reputation system
Network type	Centralized	Decentralized
Server required	Required	Not required
Network problem handling	Single point of failure, which means that the entire system crashes	Connect to another peer
Network features	Easier to implement with typical models of web-based systems	Less expensive system maintenance cost and wider network bandwidth
Reliability and integrity	Existing reviews can be manipulated and the system is less reliable	Review database is maintained by blockchain; therefore, no one can modify the reviews.

broadcasts it on the network for its validation by other miners. This newly created block is accepted and added to the blockchain only if more than 50% of miner nodes validate it. Otherwise, it is discarded. So, it enhances the security of the system and makes the blockchain immutable as a hacker will need more than 50% of computational power to temper the blockchain. It also prevents denial of service attacks on the system.

Malicious users can also pose a security threat over the proposed system, e.g., a malicious user accepts a job but does not submit or even undertake the assigned task. Due to this, the punctual workers are often deprived of rewards because the requester fails to gather enough data. Heretofore, the problem was usually solved by centralized reputation management systems; however, they penalized the workers with low reputation.

In the proposed system, this issue is tackled by communicating through smart contracts. Before the assignment of task, a worker and requester submit a designated amount of cryptocurrency, which compels both parties to perform according to the defined criteria. If in any case, a party decides to back off, the deposited amount is given to the opposite party. Furthermore, the consensus protocol ensures the correct execution of smart contracts. The combination of consensus mechanism with cryptocurrency deposit provides a fair trading mechanism for CSN.

5.2. Privacy Analysis. In this paper, we consider one of the three scenarios of privacy leakage as explained by [33]. In the proposed system, the data collectors submit their location information when they show interest in a task. The exact location submission is mandatory for effective and efficient task allocation. To tackle this problem, AES128 is used to encrypt all the information of data collectors, once they submit the private details. As the system is based on blockchain, all the workers execute the assigned jobs anonymously. However, even if a worker's identity is reidentified, the attacker still has no clue about the worker's exact location.

Based on the above analysis, we claim that our proposed system model effectively prevents the location privacy disclosure of workers in CSN.

5.3. Robustness Analysis. In the proposed system, we have used the Ethereum platform for deploying three smart contracts. The robustness analysis is elaborated in the subsections below.

5.3.1. Ethereum Platform Robustness. Ethereum is an open-source blockchain-based platform for building decentralized applications and for running smart contracts. There are multiple features of Ethereum, which make it robust. These features are stated below.

- (i) It has an unchanging nature, which means that an outsider cannot roll back any information or improvement in it
- (ii) It is secure because of the use of cryptocurrency and hashing that ensures the prevention of hacking and deceitful exercises
- (iii) It has zero downtime, the applications running on Ethereum never go down or cannot be turned off

5.3.2. Blockchain Robustness. Blockchain claims an in-built robust mechanism, and the following points ensure the robust nature of blockchain.

- (i) The blockchain technology cannot be controlled by a single authority
- (ii) It has no single point of failure threat

5.3.3. Smart Contract Robustness. Smart contracts help the system to exchange shares, property, cash, or something very important explicitly and in a conflict-free manner; thereby, avoiding any kind of third-party services. The features, which make a smart contract robust in nature, are stated below.

- (i) The execution of a smart contract is managed by the network and not by an entity, also they are not dependent on any third party so there is no danger of manipulation
- (ii) The documents are unit encrypted, which are shared on an open ledger; therefore, there is no chance of document loss
- (iii) Due to the use of cryptography, there is no chance for a contract to be hacked

6. Experimental Results

To analyze the performance of the proposed system with two communication paradigms, we have used the following tools to develop our application.

- (i) *Ganache*. It is used to deploy and maintain a personal Ethereum blockchain
- (ii) *Metamask*. It is used as an overpass that allows a computer to run blockchain based applications in the web portal without implementing a full Ethereum node
- (iii) *Vs Code*. It is used as a source code editor and solidity is used for writing the smart contracts

6.1. *Specifications*. The specifications of the system are as follows. It is a 7th Generation Intel Core i3 with 500 GB of storage and 4 GB RAM. The proposed model is evaluated using the following performance parameters.

- (i) The gas consumed by the smart contracts
- (ii) Mining time against different string input lengths of the review system
- (iii) Gas consumption against different string input values of the review system
- (iv) The comparison of execution time between different cryptographic techniques

In Table 6, gas consumption of each function is given in detail along with cost in ethers and dollars. In order to calculate the total cost in gwei, Equation (1) [29] is used.

$$\text{Total Cost}_{\text{gwei}} = \text{Gas Used} \times \text{Gas Cost}. \quad (1)$$

The standard gas price is set at 10 gwei for the smart contract cost test. Each function consumes a different amount of gas; therefore, every function has obtained a different cost.

In Figure 4, the requester's gas consumption is illustrated graphically for each and every function of smart contracts. A requester executes three functions, i.e., `CreateTask()`, `Abort()`, and `CheckData()`. In the CSN, the service provider is the initiator of the task and it acts as a requester. It is obvious from the graphs that in both smart contracts, transaction gas is consumed more as compared to the execution gas of all functions. When the transactions are verified and hoarded in the blockchain, the utilized gas is called transaction cost. Whereas the cost of execution gas is based on the execution of each and every line of source code.

The `CreateTask()` function is used to create a task along with the decided monetary reward for each sensing task. A small amount is deposited by a service provider while initiating a smart contract. The deposited amount defines the reward for the published task. Because of this, `CreateTask()` has used the greatest quantity of gas in comparison with the other operations. Whereas, `Abort()` is called, when it is believed that data collectors have gathered enough data by examining the number of data through calling the `CheckData()` function.

Figure 5 displays the gas consumption of the functions that are triggered by data collectors. In a classic CSN, the data collectors are provided with a choice regarding the selection of task. However, in the proposed scenario, it is presupposed

that the worker is looking forward for the broadcasted task only. There are two functions executed by data collectors, i.e., `getTask()` and `commitTask()`, respectively. To read the informational aspects of the task prescribed by the service provider, the `getTask()` function is used. It includes monetary reward and amount of data. Also, it is vital for workers to first look at the assignment and inspect the criteria. Otherwise, if the entered data is not according to the defined criteria, the worker is considered ineligible for incentive. Further, the `commitTask()` is called to acknowledge the gathered data that demands more computational efficiency in comparison to view the assignment; therefore, the consumed gas of former function is less in comparison to the latter function.

Figure 6 shows the gas consumption of the functions executed by the service consumer. The functions executed by smart contract are `ServiceRequest()`, `Payment()`, and `ServiceResponse()`. The first two functions consume almost the same amount of gas; however, `Payment()` demands more execution and transaction gas. This function triggers the smart contract's payment protocol. The monetary transaction takes place and later on added in the blockchain. This action justifies the increased consumption of gas.

Figure 7 depicts the gas consumption by four functions of the review system. `SetReviews()` consumes a noticeably greater amount of transaction and execution gas as compared to others. Whereas, `GetReviews()`, `GetRatings()`, and `IsReviewExist()` functions have lesser gas cost. Execution cost depends on the computational operation that is executed as an outcome of the transaction. The operations performed for `SetReviews()` are more logically complex because when this function is called, it registers the reviews of the user and saves them in blockchain for future use. However, transaction gas is the cost of sending the contract code to the Ethereum blockchain in addition to the execution cost, which validates the high transaction cost of `SetReviews()` function in comparison to others.

Figure 8 shows the mining time against each input string value of the reviews. The data is processed as inputs string for the specified fields. To investigate the effect of the size of input over the mining time, we take data in all three fields of the review system and mine to check the effect of input string size over the mining time. The result is different for all of the input strings; therefore, it is concluded that there is no explicit relationship between string size and mining time. However, the mining time depends on the network parameters of the system, as miners calculate hash, which should be below the target. Target is computed from the difficulty, which is a value set by the network to regulate it that how much it is difficult to mine a block of transactions in the blockchain. Hence, this proves that mining time is determined by network conditions.

Figure 9 demonstrates the gas consumption against the input string length. As it can be seen that on the x -axis, we have taken the input string, and on the y -axis, we have plotted gas consumption. To check whether increasing the input string increases the gas consumption, we took four input values with different string lengths. The plotted results show that they have a direct relationship as the gas consumption increases with the increase in string length.

TABLE 6: Smart contract functions cost test.

Functions	Transaction gas	Execution gas	Cost (ethers)	Cost (dollars)
IsReviewExist()	23740	790	0.0000079	0.0017
GetReview()	24476	1769	0.00001769	0.0037
GetRating()	20367	1669	0.00001669	0.0035
SetReview()	59362	34442	0.00034442	0.072
CreateTask()	857894	607038	0.00607038	1.27
Abort()	21693	11421	0.00011421	0.042
CheckData()	557894	121693	0.00121693	0.26
commitTask()	70190	47510	0.00047510	0.10
getTask()	176930	130373	0.00130373	0.27
ServiceRequest()	22875	12831	0.00012831	0.027
ServiceResponse()	23130	15381	0.00015381	0.032
Payment()	57894	21693	0.00021693	0.046

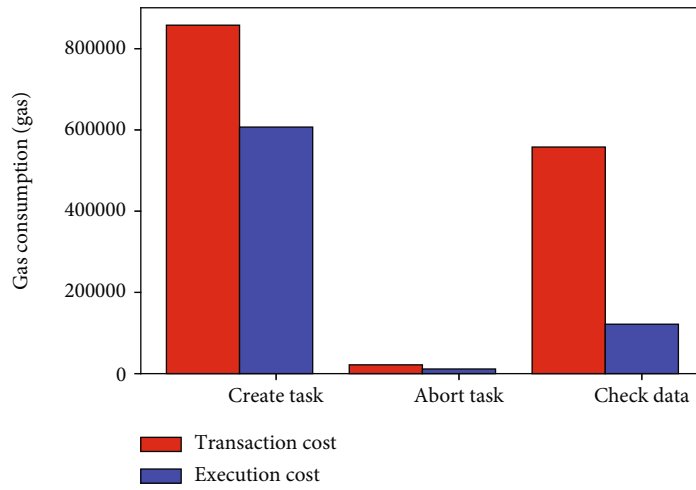


FIGURE 4: Gas consumption of service provider.

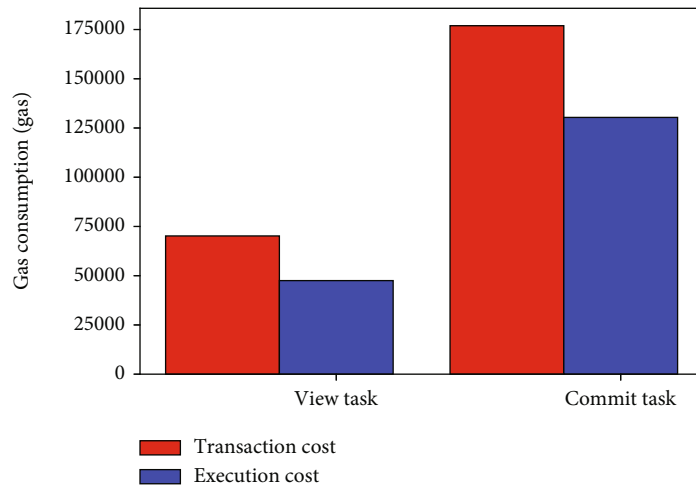


FIGURE 5: Gas consumption of data collector.

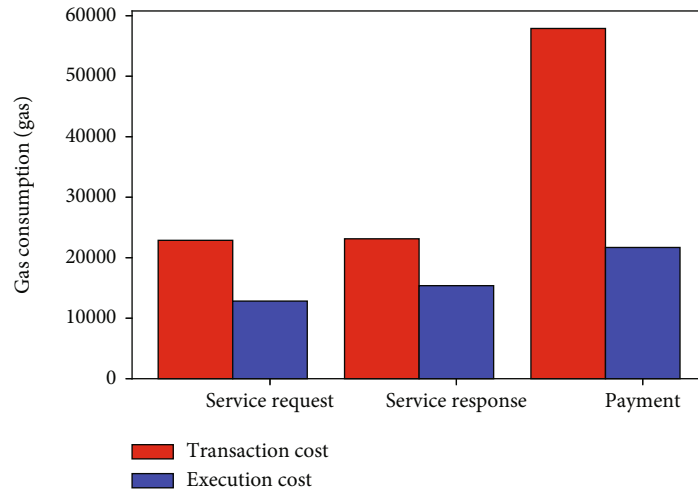


FIGURE 6: Gas consumption of service consumer.

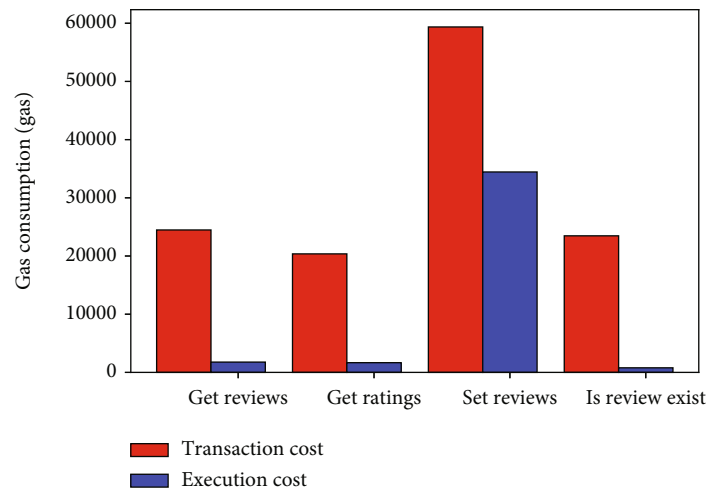


FIGURE 7: Gas consumption of review system smart contract.

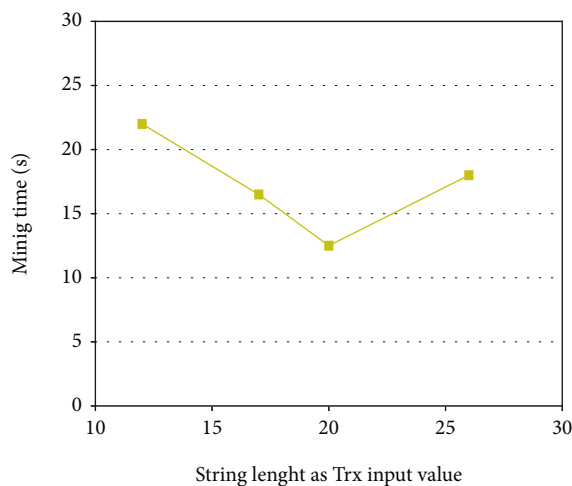


FIGURE 8: Mining time with different input values.

Figure 10 shows the comparison of cryptographic techniques based on the execution time of encryption and decryption in milliseconds (ms). The process of transforming normal text into ciphertext is called encryption; whereas the process of converting the ciphertext into normal text is called decryption. To produce a more quicker and responsive system, both of the abovementioned processes are required to take less time for execution. Similarly, they also affect the performance of the system. Therefore, for this scenario, affine cipher, 3DES, AES128, and AES256 are compared based on execution time. Affine cipher is used in [2] for protecting the location information of workers; however, it is affiliated with the class of classical monoalphabetic substitution schemes. The mentioned class can be easily interpreted by solving a set of concurrent equations. Additionally, it is liable to all the cipher attacks; as a consequence, it is not considered to be a strong and secure technique for encryption in comparison to the modern symmetric key block cipher approaches. From the literature review of [22, 26, 27], we executed three more encryption techniques. The execution time noted for affine cipher, AES256, AES128, and 3DES is 9.07,

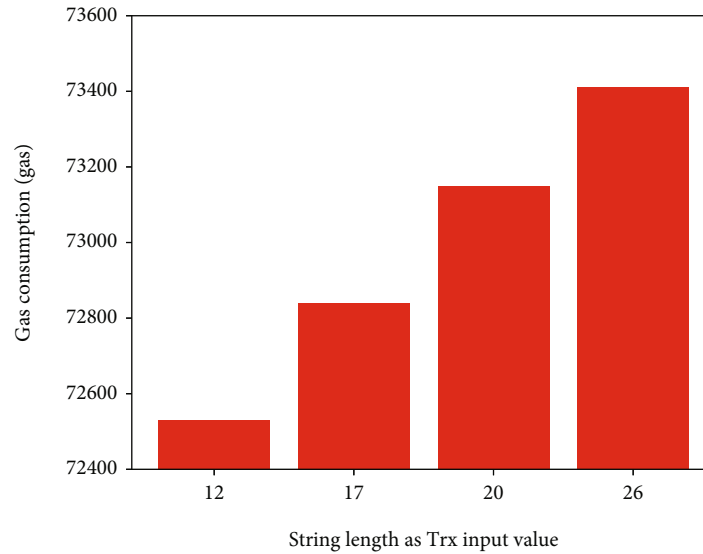


FIGURE 9: Gas consumption against different input values.

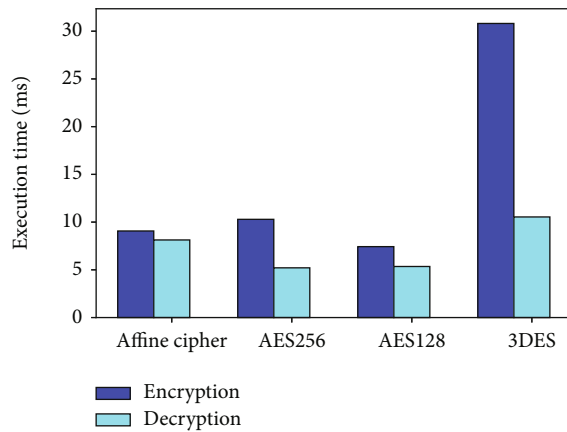


FIGURE 10: The comparison of execution time for affine cipher, AES256, AES128, and 3DES.

10.29, 7.43, and 30.81, respectively. By acquiring the time, it is found that AES128 performs better with the least execution time in comparison to AES256, affine cipher, and 3DES. AES256 is considered to be more secure when compared with AES128 having more rounds and lengthy key size, i.e., 256 bits. However, AES128 beats the AES256 in terms of execution time. Hence, to have a more responsive mechanism, we preferred AES128 over AES256 according to the suitability of the proposed scenario.

7. Conclusion and Future Work

With the evolution and expansion of technology on a huge scale, blockchain has come forth as the most suitable solution for providing a distributed yet shared environment while preserving the privacy of all the participants in the applications. In this article, a decentralized incentive and reputation system is proposed for a CSN. It is aimed at persuading workers and at captivating expert user's attention. The process of encryption is incorporated to protect the private

information of data collectors. Smart contracts are used as a reliable transmission medium. The proposed system caters to the requirements of all entities in a decentralized manner; consequently achieving consistent data, secure communication, increased cooperation rate, and authentic reviews. The incentive mechanism is evaluated by inspecting the gas utilization of all the functions, whereas the reputation mechanism is inspected through studying the gas consumption and mining time against input string length. Furthermore, based on encryption's execution time, i.e., 7.43 ms for AES128 and 9.07 ms for affine cipher, the former technique is selected for the proposed scenario. Although AES256 provides a high level of security as compared to AES128; however, AES256 takes more time to encrypt. Therefore, the trade-off between time and security level is also considered for the proposed scenario, and it is concluded that AES128 is an appropriate technique for the system.

For the future, our goal is to measure the trustworthiness of the data, which is submitted by the participants. The objective is to compare the user's trust attributes and the application of nonparametric statistic methods and analyze the outcome. The results will be examined based on data subjectivity for the proposed scenario.

Data Availability

No data has been used for this work.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the MSIT (Ministry of Science and ICT, South Korea), under the ITRC (Information Technology Research Center) support program (IITP-2021-2016-

0-00313) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

- [1] D. He, S. Chan, and M. Guizani, "User privacy and data trustworthiness in mobile crowd sensing," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 28–34, 2015.
- [2] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "Incentive mechanism for privacy-aware data aggregation in mobile crowd sensing systems," *IEEE/ACM Transactions on Networking*, vol. 26, no. 5, pp. 2019–2032, 2018.
- [3] G. Merlino, S. Arkoulis, S. Distefano, C. Papagianni, A. Puliafito, and S. Papavassiliou, "Mobile crowdsensing as a service: a platform for applications on top of sensing clouds," *Future Generation Computer Systems*, vol. 56, pp. 623–639, 2016.
- [4] J. Nie, J. Luo, Z. Xiong, D. Niyato, and P. Wang, "A Stackelberg game approach toward socially-aware incentive mechanisms for mobile crowdsensing," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 724–738, 2019.
- [5] S. Gisdakis, T. Giannetos, and P. Papadimitratos, "Security, privacy, and incentive provision for mobile crowd sensing systems," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 839–853, 2016.
- [6] C. Luo, X. Liu, W. Xue et al., "Predictable privacy-preserving mobile crowd sensing: a tale of two roles," *IEEE/ACM Transactions on Networking*, vol. 27, no. 1, pp. 361–374, 2019.
- [7] W. Ahmad, S. Wang, A. Ullah, Sheharyar, and M. Y. Shabir, "Reputation-aware recruitment and credible reporting for platform utility in mobile crowd sensing with smart devices in IoT," *Sensors*, vol. 18, no. 10, p. 3305, 2018.
- [8] N. D. Lane, S. B. Eisenman, M. Musolesi, E. Miluzzo, and A. T. Campbell, "Urban sensing systems: opportunistic or participatory?," in *Proceedings of the 9th workshop on Mobile computing systems and applications - HotMobile '08*, pp. 11–16, Napa Valley California, USA, February 2008.
- [9] G. Yang, S. He, Z. Shi, and J. Chen, "Promoting cooperation by the social incentive mechanism in mobile crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 86–92, 2017.
- [10] K. Ota, M. Dong, J. Gui, and A. Liu, "QUOIN: incentive mechanisms for crowd sensing networks," *IEEE Network*, vol. 32, no. 2, pp. 114–119, 2018.
- [11] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raji, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet of Things Journal*, vol. 2, no. 5, pp. 370–380, 2015.
- [12] O. Samuel and N. Javaid, "A secure blockchain-based demurrage mechanism for energy trading in smart communities," *International Journal of Energy Research*, vol. 45, no. 1, pp. 297–315, 2021.
- [13] O. Samuel, A. Almogren, A. Javaid, M. Zuair, I. Ullah, and N. Javaid, "Leveraging blockchain technology for secure energy trading and least-cost evaluation of decentralized contributions to electrification in Sub-Saharan Africa," *Entropy*, vol. 22, no. 2, p. 226, 2020.
- [14] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, "A blockchain based load balancing in decentralized hybrid P2P energy trading market in smart grid," *IEEE Access*, vol. 8, pp. 47047–47062, 2020.
- [15] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: a complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020.
- [16] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Applied Sciences*, vol. 10, no. 2, p. 488, 2020.
- [17] Z. Noshad, A. Javaid, M. Zahid, I. Ali, and N. Javaid, "A blockchain based incentive mechanism for crowd sensing network," in *the 14th international conference on P2P, parallel, grid, cloud and internet computing*, pp. 568–578, Springer, Cham, 2019.
- [18] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018.
- [19] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, 2018.
- [20] J. Huang, L. Kong, L. Kong, Z. Liu, Z. Liu, and G. Chen, "Blockchain-based crowd-sensing system," in *2018 1st IEEE international conference on hot information-centric networking (HotICN)*, pp. 234–235, Shenzhen, China, August 2018.
- [21] M. Dai, Z. Su, Y. Wang, and Q. Xu, "Contract theory based incentive scheme for mobile crowd sensing networks," in *2018 international conference on selected topics in Mobile and wireless networking (MoWNeT)*, pp. 1–5, Tangier, Morocco, June 2018.
- [22] G. Cardone, A. Corradi, L. Foschini, and R. Ianniello, "Participat: a large-scale crowdsensing platform," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 21–32, 2016.
- [23] P. A. Mottur and N. R. Whittaker, "Vizsafe: the decentralized crowdsourcing safety network," *2018 IEEE international smart cities conference (ISC2)*, 2018, pp. 1–6, Kansas City, MO, USA, 2018.
- [24] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2958–2970, 2017.
- [25] Z. Chi, Y. Wang, Y. Huang, and X. Tong, "The novel location privacy-preserving CKD for mobile crowdsourcing systems," *IEEE Access*, vol. 6, pp. 5678–5687, 2017.
- [26] M. M. Ahamad and M. I. Abdullah, "Comparison of encryption algorithms for multimedia," *Rajshahi University Journal of Science and Engineering*, vol. 44, pp. 131–139, 2016.
- [27] M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention," *Journal Computer Science Applications and Information Technology*, vol. 3, pp. 1–7, 2018.
- [28] B. Guo, H. Chen, Z. Yu et al., "Taskme: toward a dynamic and quality-enhanced incentive mechanism for mobile crowd sensing," *International Journal of Human-Computer Studies*, vol. 102, pp. 14–26, 2017.
- [29] J. S. Park, T. Y. Youn, H. B. Kim, K. H. Rhee, and S. U. Shin, "Smart contract-based review system for an IoT data marketplace," *Sensors*, vol. 18, no. 10, p. 3577, 2018.
- [30] K. Wang, Z. Zhang, and H. S. Kim, "ReviewChain: smart contract based review system with multi-blockchain gateway," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications*

(GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1521–1526, Halifax, NS, Canada, 2018.

- [31] S. T. Muriki, *Online Reviews Immutability Tool Using Blockchain Technology*, Tone Analyzer, 2019.
- [32] F. David, “Tone analyzer,” 2019, 2019, <https://tone-analyzer-demo.ng.bluemix.net>.
- [33] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, “A blockchain-based location privacy-preserving crowdsensing system,” *Future Generation Computer Systems*, vol. 94, pp. 408–418, 2019.

Research Article

Power Grid-Oriented Cascading Failure Vulnerability Identifying Method Based on Wireless Sensors

Shudong Li ¹, Yanshan Chen,² Xiaobo Wu ³, Xiaochun Cheng ⁴, and Zhihong Tian ¹

¹Cyberspace Institute of Advance Technology, Guangzhou University, Guangzhou 510006, China

²School of Economics and Statistics, Guangzhou University, Guangzhou 510006, China

³School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China

⁴School of Science and Technology, Middlesex University, London, UK

Correspondence should be addressed to Shudong Li; lishudong@gzhu.edu.cn and Xiaobo Wu; happywxb@gzhu.edu.cn

Received 24 April 2020; Revised 28 August 2020; Accepted 22 May 2021; Published 28 June 2021

Academic Editor: Iftikhar Ahmad

Copyright © 2021 Shudong Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In our paper, we study the vulnerability in cascading failures of the real-world network (power grid) under intentional attacks. Here, we use three indexes (B , K , k -shell) to measure the importance of nodes; that is, we define three attacks, respectively. Under these attacks, we measure the process of cascade effect in network by the number of avalanche nodes, the time steps, and the speed of the cascade propagation. Also, we define the node's bearing capacity as a tolerant parameter to study the robustness of the network under three attacks. Taking the power grid as an example, we have obtained a good regularity of the collapse of the network when the node's affordability is low. In terms of time and speed, under the betweenness-based attacks, the network collapses faster, but for the number of avalanche nodes, under the degree-based attack, the number of the failed nodes is highest. When the nodes' bearing capacity becomes large, the regularity of the network's performances is not obvious. The findings can be applied to identify the vulnerable nodes in real networks such as wireless sensor networks and improve their robustness against different attacks.

1. Introduction

Nowadays, people's daily life is increasingly dependent on electricity, but the failures and blackout happened in the electricity system has resulted in heavy losses and a huge impact on people's lives. There are a lot of famous examples like the massive power failure on the West Coast of United States in September 2011, the breakdown of Ukraine's electricity system under malicious attacks and the blackout in New York city in July 2019, and the massive power failure on the U.S. West Coast in 2019. Therefore, to this day, the research on the power grid is still hot. The current research on network robustness mainly includes these aspects: research based on power grid structure, analysis based on cascading effects, how to identify network attacks, and how to defend network attacks.

In terms of structural analysis, Huang [1] et al. (2013) used the theory of complex networks and obtained the distribution of risk energy along the path in the vulnerability anal-

ysis of cascading faults considering branch structures. Based on graph theory technology, Correa [2] et al. (2013) obtained the applicability conclusion of the graph theory method for the vulnerability of power grids by comparing the physical flow model and the statistical indicators of scale-free graphs. Based on the normalization effect of neighboring nodes and the weight distribution of nodes in the network, Wang [3] et al. (2014) studied the different roles of low-load and high-load nodes and the relationship between some parameters in the network and the strongest level of robustness. Finally, through numerical simulation, they obtained the parameter values corresponding to the model at the strongest level of robustness. Ouyang [4] et al. (2014) used the betweenness based-model (BBM), direct current power flow model (DCPFM), and purely topological model (PTM) to study network robustness under intentional attacks based on betweenness, degree, importance, and maximum traffic. Yang [5] et al. (2015) discussed the relationship between community structure and network robustness and proposed

a three-step strategy to improve network robustness while maintaining the degree distribution and the structure of the network community.

In terms of analysis based on cascading effects, considering the traffic load, Tan [6] et al. (2015) used the Barabasi-Albert scale-free network and interdependent Erdos-Renyi random graph to research the effect of the coupling mode on the cascade effect. Through research, Erdos-Renyi random graphs are fragile and robust. However, the interdependent Barabasi-Albert scale-free network is vulnerable to intentional attacks and the random attacks. These results are similar for interdependent communication networks and power grids, for the nonvulnerability under intentional attacks and the actual interdependent system. Cai [7] et al. (2016) analyzed the complex effects of cascading faults by modeling the interdependence between power systems and dispatch data networks. Their simulation results show that under random attacks, the probability of catastrophic failure of the power grid combined with the mesh structure is higher than that with a double-star structure; while under intentional attacks, the transmission performance of the mesh network is better than that of the double-star structure. Hai-PengRen [8] et al. (2016) proposed a new load distribution for the cascade effect and a node removal rule, that is, in the opposite direction of the flow, removing the first overload node, and then the network distributes the load and continues cascading process. This method has proven to suppress large-scale cascading failures. According to the maximum flow theory, Wenli [9] et al. (2016) proposed a model of cascading failure. Their results show that the node load distribution has a great impact on the cascading dynamics and the tolerance parameter threshold. Kornbluth [10] et al. (2018) use the node's betweenness centrality as the load to research the cascading effect of the network when the node's load is overloaded. They study the functional relationship between the initial attack and the number of surviving nodes at the end of the cascade PF strength under different tolerance values in Erdős-Renyi graphs and random regular graphs.

In terms of how to identify network attacks, Yan [11] et al. (2017) analyzed the vulnerability of the transmission network under sequential topology attack and proposed a method based on Q-learning. This method can identify the critical attack sequence considering the dynamic behavior of the physical system. Wang [12] et al. (2017) developed a smart search method based on state-space pruning to identify incidents of cyber attacks. They used the stochastic chemistry method and particle swarm optimization algorithm and took the IEEE system as an example to verify the efficiency and of the method. Lei [13] et al. (2020) proposed a distributed iterative positioning algorithm based on the abandonment strategy of the sensor relative to its neighbor's center of gravity coordinates. The algorithm uses relative distance calculations to locate the data packet loss through the neighbor's communication link. And they accurately locate the sensor through this algorithm. Daniel [14] et al. (2020) proposed an algorithm that shows the relationship between the variance of the attacker's signal and how far away the nodes are, which solves the problem of constructing a cen-

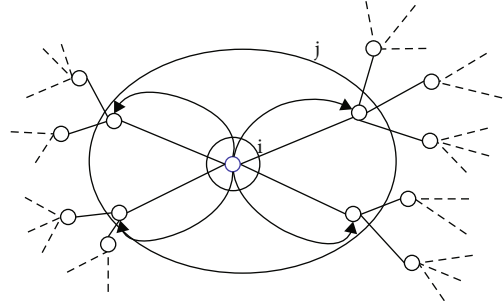


FIGURE 1: The evolution process of cascading faults in the network model.

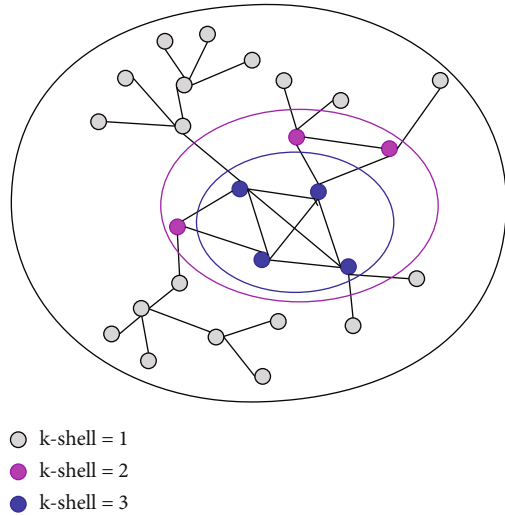


FIGURE 2: The definition of k -shell. Removing all the nodes with degree 1 and repeating this step until there are no nodes with degree 1 in the grid. Then, define their value of k -shell as 1 (k -shell = 1), which is the outer circle in the figure. Next, continue to remove the node with a degree of 2. As described above, the k -shell value of the removed nodes is defined as 2 (k -shell = 2), which is circle 2. Similarly, the k -shell values of all points are obtained.

tralized and distributed version of Nesterov with the best fixed parameters.

In terms of how to defend network attacks, Zheng [15] et al. (2014) proposed a weighting strategy for edges, that is, designing the path length of the edge as the product of the clustering coefficients of the edge nodes and calculating the corrected neutrality center of the edge and applying it as a weight to the cascade model. It is found that the weighting scheme based on the modified betweenness centrality makes the three networks of the modular network, scale-free network, and small-world network all better than the original betweenness centrality networks that are more robust against edge attack. Liu [16] et al. (2015) found two ways to reduce the system vulnerability: (1) protect nodes with high degree and (2) increase the degree of correlation between networks. Guo [17] et al. (2017) proposed a vulnerability analysis method using the Cyber-Physical Power System (CPPS) model composed of the physical layer, network layer, and network physical interface and used this method to calculate

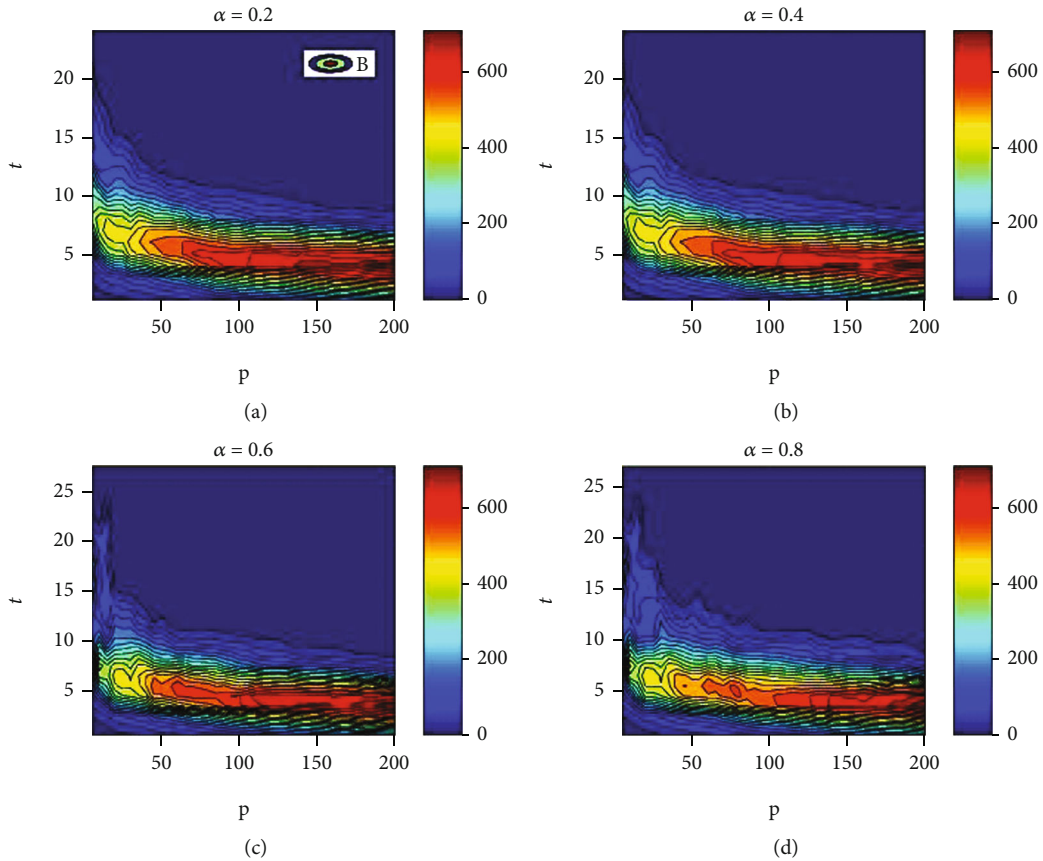


FIGURE 3: Under B attack, the figure shows how many nodes failed in the network (color shades) at time t (axis Y) when p nodes were attacked (axis X), where the range of p is 5 to 200, with an interval of 5 nodes. (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

the performance index of the model before and after the cascade failure. By comparing different attack strategies and interface strategies, they concluded that CPPS should protect high-indexed nodes and is more vulnerable to malicious attacks. Wang [18] et al. (2018) proposed a strategy to defend against cyber attacks by studying electronic computing physical systems (ECPs). Besides, they also provided a weight adjustment strategy to work out the problem of unbalanced current caused by the split event. In the paper, their assessment of vulnerability has five aspects: robustness, economic cost, degree of damage, fragile equipment, and trigger points. Ma [19] et al. (2019) proposed a scale-free network model that can more effectively control the propagation of cascading faults. In their model, the connection load of any two nodes is defined, taking into account the degree and intermediateness of the nodes. Irshaad [20] et al. (2019) combined cognitive dynamic and state estimation systems in the smart network and proposed a new SG metric: entropy state. The manager achieves the goal of improving the entropy state by reconfiguring the weights of the sensors in the grid and dynamically optimizing the state estimation process. And CDS is the best choice for monitoring systems.

It can be seen from the above literature review that scholars understand the network structure and cascading effects and use sensors to identify attacks and defend them. In this article, we default to the identification of sensors

and attach importance to defense to protect high-load nodes. However, rather than studying structural defenses, we value the impact of the network after an attack. We recorded not only the number of nodes in the network that crashed but also the speed and time of the crash. Because we believe that under the technical recognition of sensors, understanding the law of network collapse is of great practical significance for future defenses.

We break this article into three sections. In Section I, we will introduce the load distribution model of the network. In Section II, we will show three attacks. In Section III, we will list some indicators to show the extent to which the network is crashing. In Section IV, we will present the results graphically and analyze them. Finally, we will give the conclusion.

2. Results and Discussion

2.1. The Cascading Failure Model

2.1.1. Load Distribution Model. It can be seen from multiple studies that the load of a node is often estimated by the node's betweenness centrality [21, 22]. Therefore, in our paper, we set the betweenness centrality of the node as its load.

In reality, when a node is crashed by an attack, its load is distributed to other nodes in the network [23]. There are two distribution methods, global distribution and local

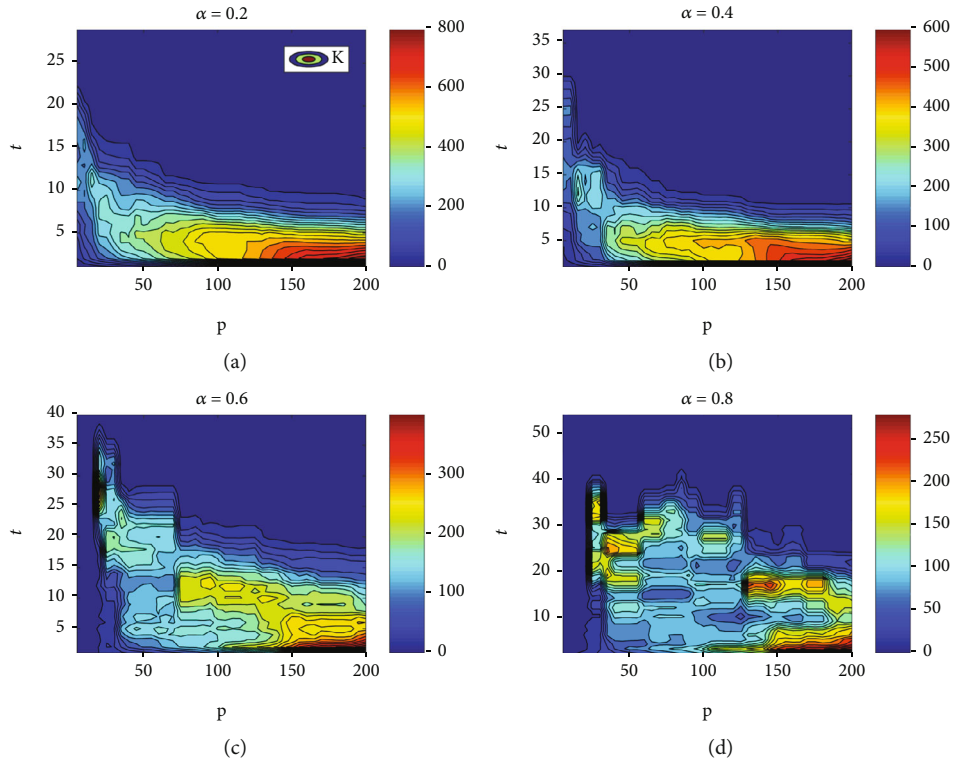


FIGURE 4: Under K attack, the figure shows how many nodes failed in the network (color shades) at time t (axis Y) when p nodes were attacked (axis X), where the range of p is 5 to 200, with an interval of 5 nodes. (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

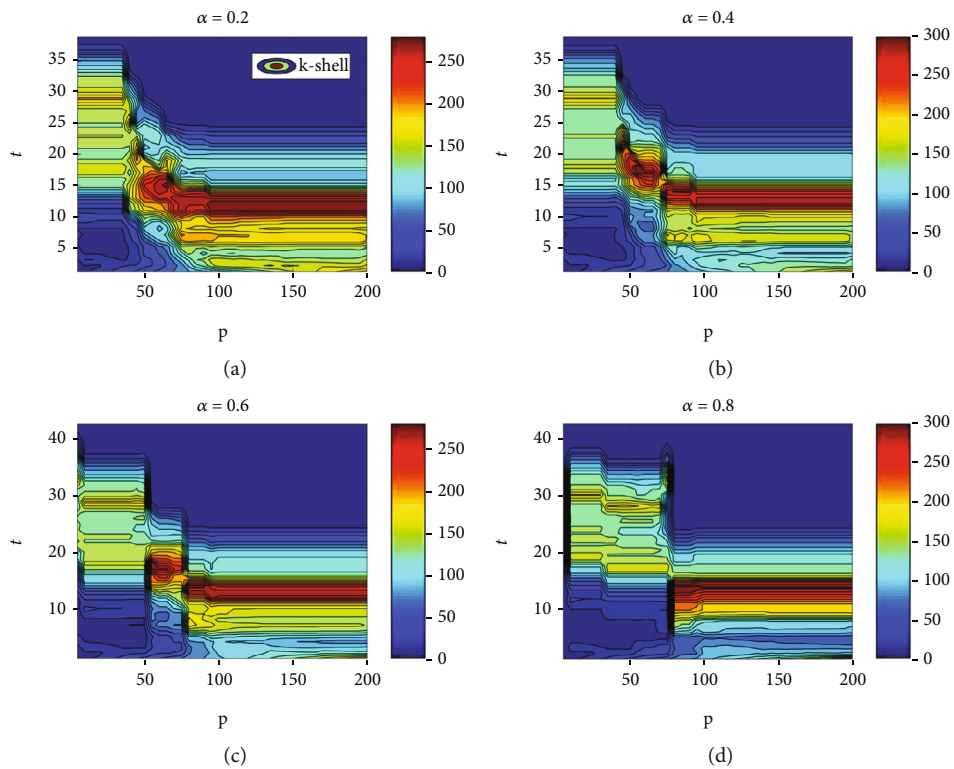


FIGURE 5: Under k -shell attack, the figure shows how many nodes failed in the network (color shades) at time t (axis Y) when p nodes were attacked (axis X), where the range of p is 5 to 200, with an interval of 5 nodes. (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

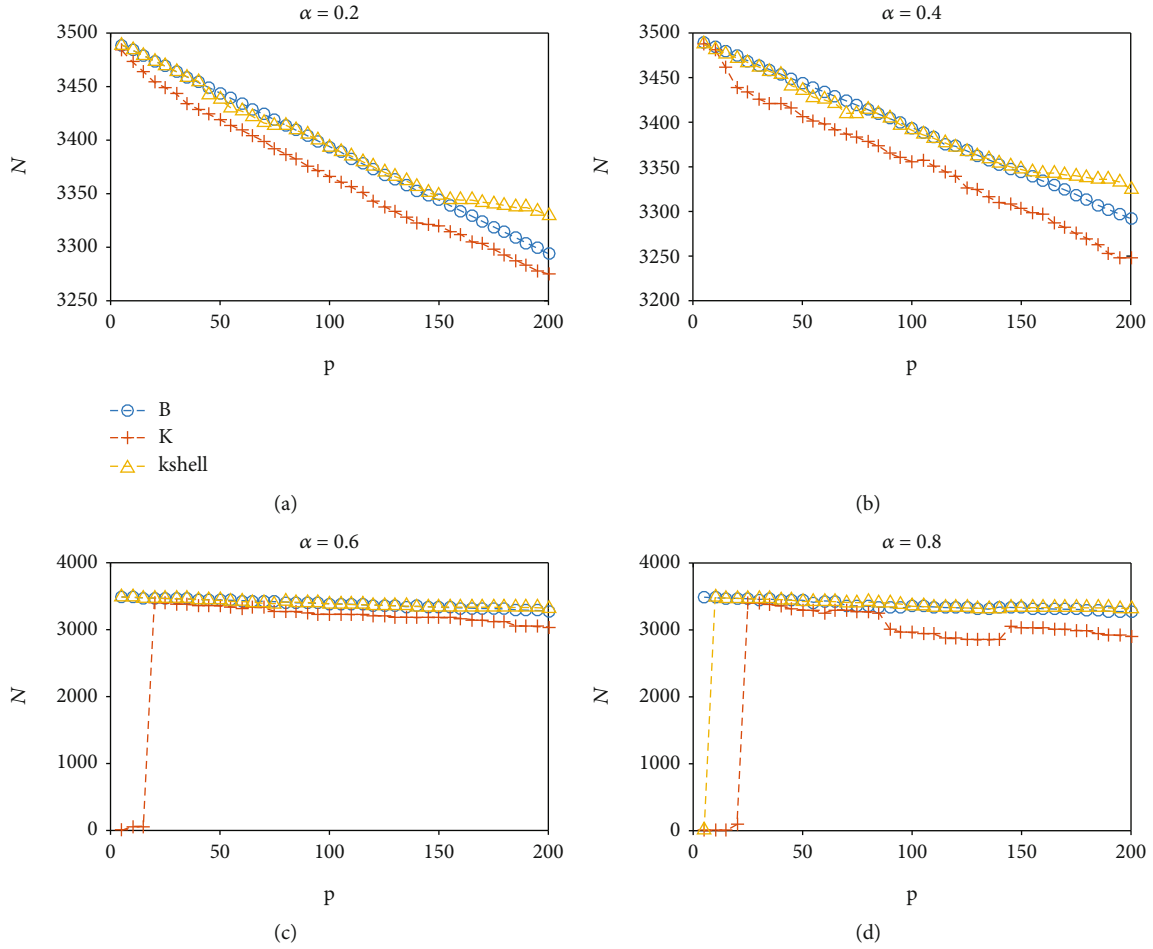


FIGURE 6: Under three attack strategies, the total number of the failed nodes N (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

distribution. Global distribution seems to be more comprehensive, but in actual research, global distribution calculation is huge, and in global distribution, the load is distributed in inverse proportion to the distance. On the contrary, distributing load to neighboring nodes is effective and reasonable. On the one hand, it can show the level after the collapse of the network. On the other hand, calculations are greatly reduced. Local distribution is not single, for example, using game theory [24]. Consequently, we adopt the local distribution method of node load distribution to its neighboring nodes after a node fails in this article, which is more suitable for research.

As shown in Figure 1, when the node i crashes, it allocates its own load to its neighboring node set j in a certain form. When a node is a neighboring node that exceeds its maximum load, the node fails and continues to be distributed to its neighboring nodes, which results in the cascade effect. Until the assigned nodes in the network do not exceed the maximum load, the process of cascading faults stops [25].

2.1.2. Cascade-Related Indicators. To measure the cascading effect of the network, you need to define some relevant indicators.

First of all, as mentioned above, we define the initial load (L) of node i [26] as the node's betweenness centrality (B).

$$L_i(0) = B_i. \quad (1)$$

Secondly, define the maximum load (C) that the node can withstand [27]. The definition is as follows:

$$C_i = (1 + \alpha)L_i(0). \quad (2)$$

In the formula, α is a tunable parameter, ranging from 0 to 1, indicating the performance of the nodes [28]. The larger the value of α , the better the load-carrying capacity of the node.

The next is how to distribute. At time t , as node i failed, its neighboring node k increases the load (ΔL_k) as

$$\Delta L_k(t) = \frac{B_i}{\sum B_j} L_i(t-1), \quad (3)$$

where k is any node of set j . The load distributed from the node i is added to each neighboring node. If the one of neighboring nodes exceeds its maximum load, the node fails [29].

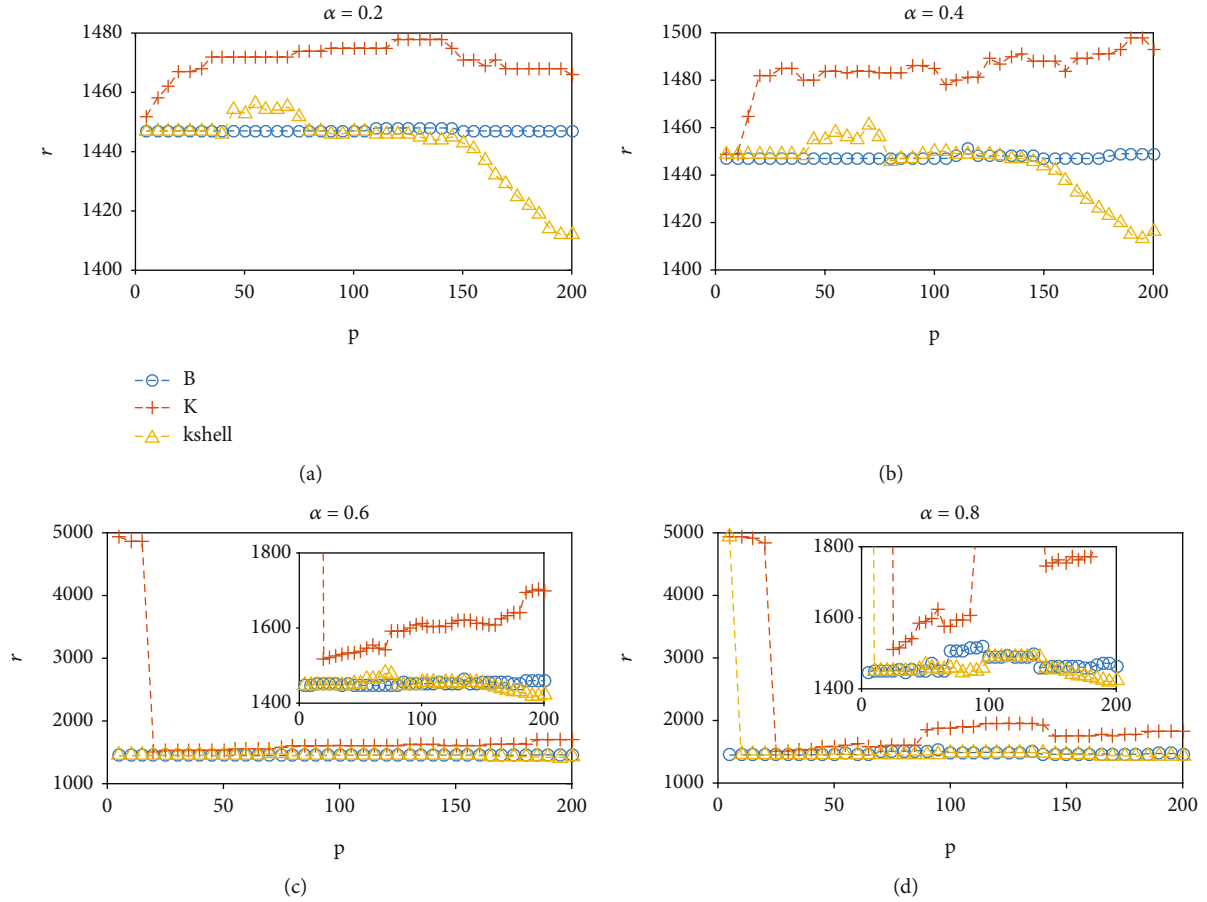


FIGURE 7: Under three attack strategies, the number of remaining nodes r (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

2.1.3. Simulated Attack Model. In general, our model is to achieve intentional attacks in reality by selecting high-load nodes to attack. After being attacked, the attacked node will distribute its load to neighboring nodes, that is, using the previous load distribution model. When any neighboring node's load exceeds its capacity, it will collapse and continue to distribute its load, thus form a series of chain reactions [30, 31]. And we will simulate this process through a computer to get our final conclusion.

2.2. Three Attack Strategies. We examine the survivability of the network under intentional attacks [32] in this article. Under intentional attacks, important nodes in the network will be attacked. Important nodes are often measured by the node's betweenness centrality, degree [33], k -shell [34] value, etc. Therefore, we study three attacks that sort these three metrics in descending order to attack. The three attacks are as follows:

- (1) Betweenness attack (B attack): based on the above-mentioned distribution method, we sort all nodes in descending order of the betweenness centrality, then attack the top nodes
- (2) Degree-based attack (K attack): The nodes to be attacked are arranged in descending order of degrees,

and the rest are the same as the betweenness-based attack

- (3) k -shell-based attack: keep the other conditions the same and arrange the attacked nodes in descending order according to the value of k -shell. For the definition of k -shell, see the Figure 2 below

Attack the nodes according to these three attacks, and then through certain indicators [35], we can see the degree of network collapse. Next, we will introduce the evaluation indicators.

2.3. Evaluation Indicators. Obviously, the degree of network collapse [36, 37] is bound up with the number of nodes that fail. The quantity available is an important indicator. On the other hand, due to the cascading effect, the moments when different nodes fail are not necessarily the same. Therefore, we must first define the time of the cascade. With quantity and time, we naturally think of another indicator—speed. Below, we will explain these three indicators in detail.

- (1) Time: As for the time, we define the time of the attack as the moment 0 ($t = 0$), the time of the neighboring nodes fail caused by the attacked nodes as the moment 1 ($t = 1$), and so on to define the cascade moment. In addition, what we can get from this is

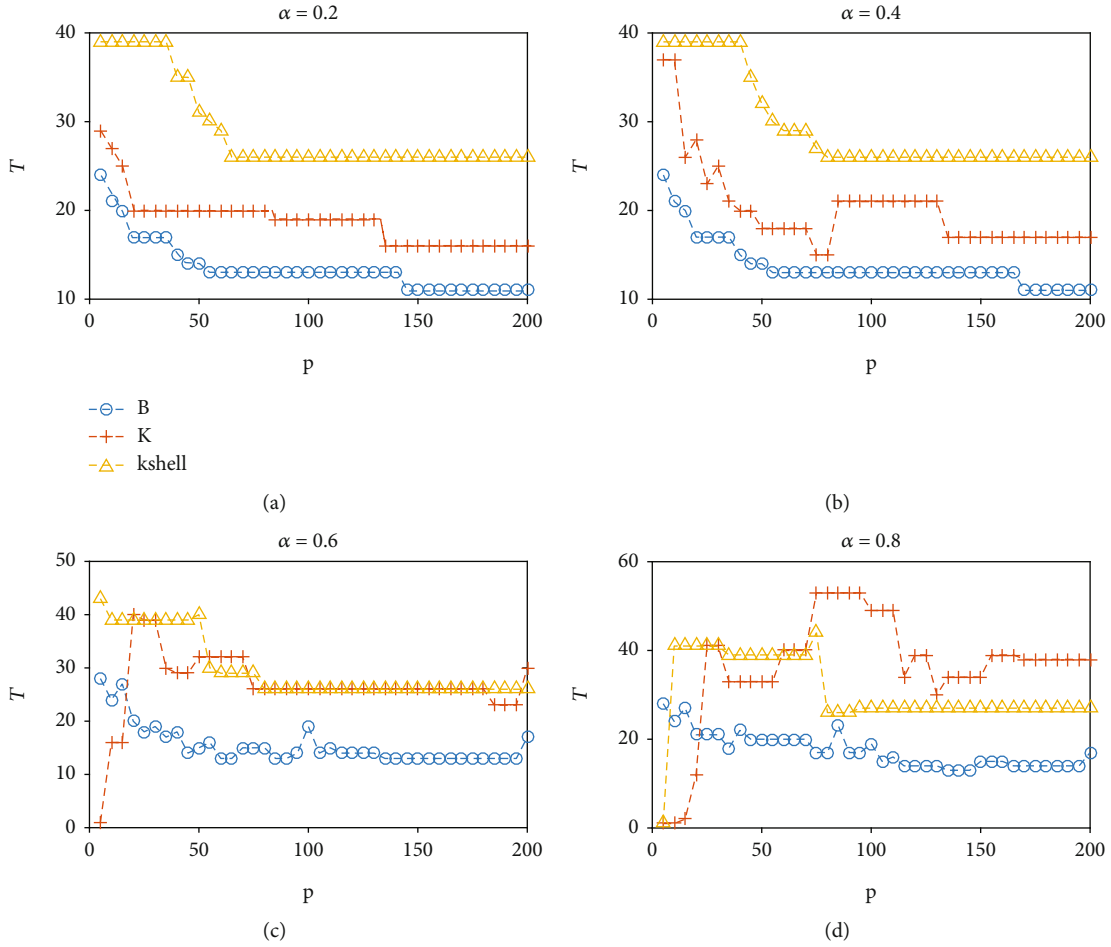


FIGURE 8: Under three attack strategies, the persistent time of cascade T (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

that the last moment recorded is the time (t) used for the cascade effect

- (2) The number of failed nodes: Aiming to analyze the collapse of the network in the cascade effect process, we count the nodes that fail at different times ($n(t)$). By adding these numbers, we can get the total number of nodes that fail, calculated as follows:

$$N = \sum_{t=1}^T n(t). \quad (4)$$

- (3) The number of noncrashed nodes: Knowing the total number of nodes (M) in the power grid and the number of failure nodes, we can easily calculate the nodes that did not fail, excluding the number of nodes that have attacked (p), calculated as follows:

$$r = M - N - p. \quad (5)$$

- (4) Speed of cascade: Speed is the quotient of quantity (N) and time (t). Here, the time it takes for the cascade effect to start and end. The quantity (N) here refers to the total number of nodes that fail. The specific formula is as follows:

$$v = \frac{N}{T}. \quad (6)$$

All in all, it is easy to know that the total number of failure nodes shows the degree of network collapse, and time and speed show the effects of different attacks. Then, based on these indicators, from the results, we can detect the effect of the cascade effect of the network under different attack conditions.

3. Result Analysis

Based on the previous model and evaluation indicators, we test it using the U.S. grid as an example. This power grid is a network with 4941 nodes and 6,594 edges. Here, we assume

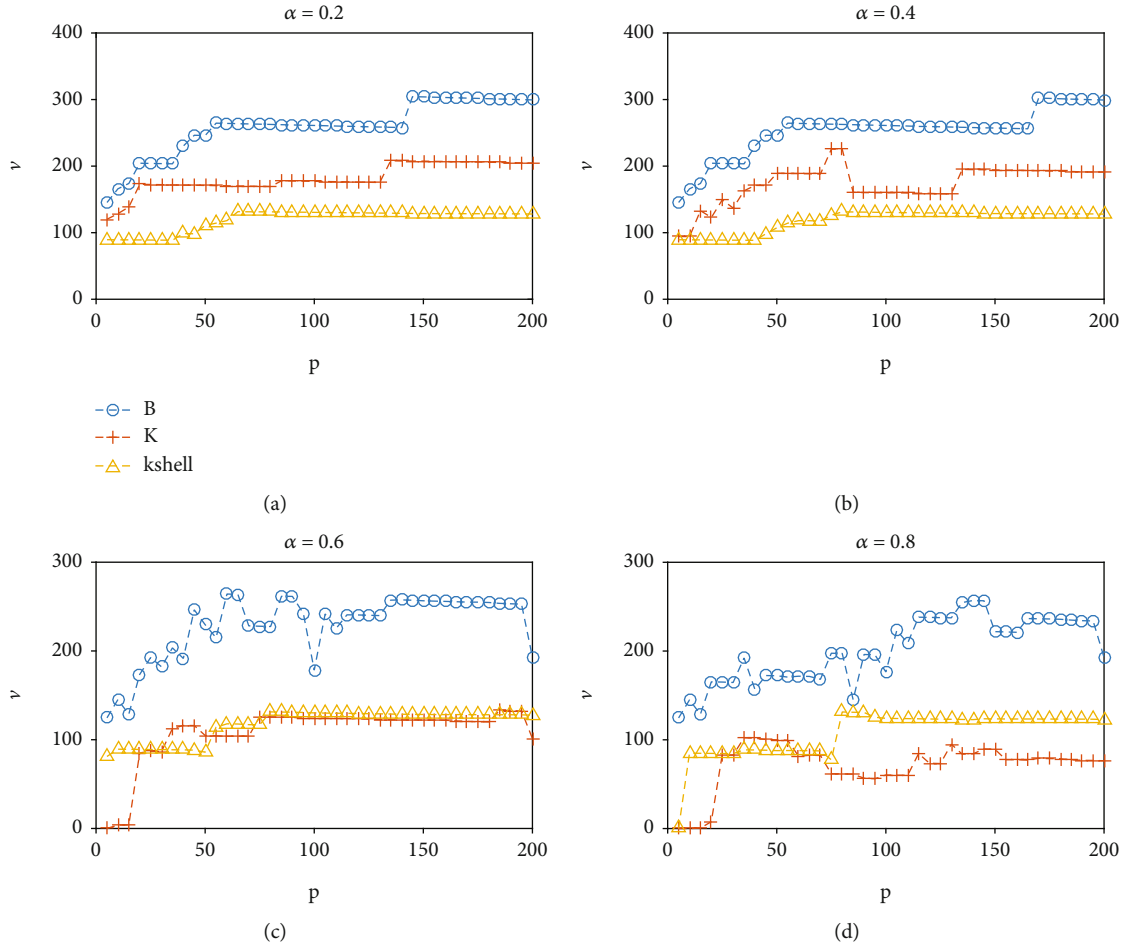


FIGURE 9: Under three attack strategies, the speed of cascade effect V (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

that the edges of the network [38] are unweighted, and the distribution of the load is undirected.

3.1. Preliminary Analysis. As mentioned above, we will record the number of nodes that fail at each moment in the cascade effect. Therefore, we will initially display it in a three-dimensional graph.

Through the adjustment of α and the adjustment of attack nodes, we can have different results. Among them, we will find some novel conclusions. Next, we will present them in turn.

As can be seen from the vertical perspective of Figure 3, under the B attack, the number of nodes in the cascade effect increases with time, showing a trend of increasing first and then decreasing. From the horizontal perspective, as the number of attacked nodes increases, so does the number of collapse nodes in the cascade effect. And it can be roughly seen that with the increasing of the number of attacked nodes, the total time of the cascade effect generally decreases.

Next, we use the same distribution method to perform the same operation on nodes sorted by degree (K). The result is shown in Figure 4.

It can be seen from Figure 4 that the horizontal and vertical images are roughly the same as the B attacks, but in the

K attack, when the node performance is good, that is, when α is large, attacking a few important nodes has little impact on the entire network.

At last, we use the k -shell to measure the importance that is sorted by k -shell, attack the node with a large value of k -shell, and use the same distribution method to record the number of failure nodes, as shown in Figure 5.

It can be seen from Figure 5 that the image in the horizontal and vertical directions is roughly the same as the two modes, but compared to the previous two attack mode, this attack mode has a large time span and shows a fault phenomenon, as shown in Figure 5(a). The first 40 attacked nodes and less than 40 show roughly the same effect on the network, but when the number of attack nodes is greater than 40, the result of the attack is significantly different. This may be related to the point ordering with the same k -shell value.

3.2. Advanced Analysis. When α is determined, in a three-dimensional graph, we can know the time of the crash (t) and the number of crashed nodes at different times ($n(t)$) and compare the network crashes that attacked different numbers of nodes. However, we do not know whether the final total number of crashed nodes (N) still has such

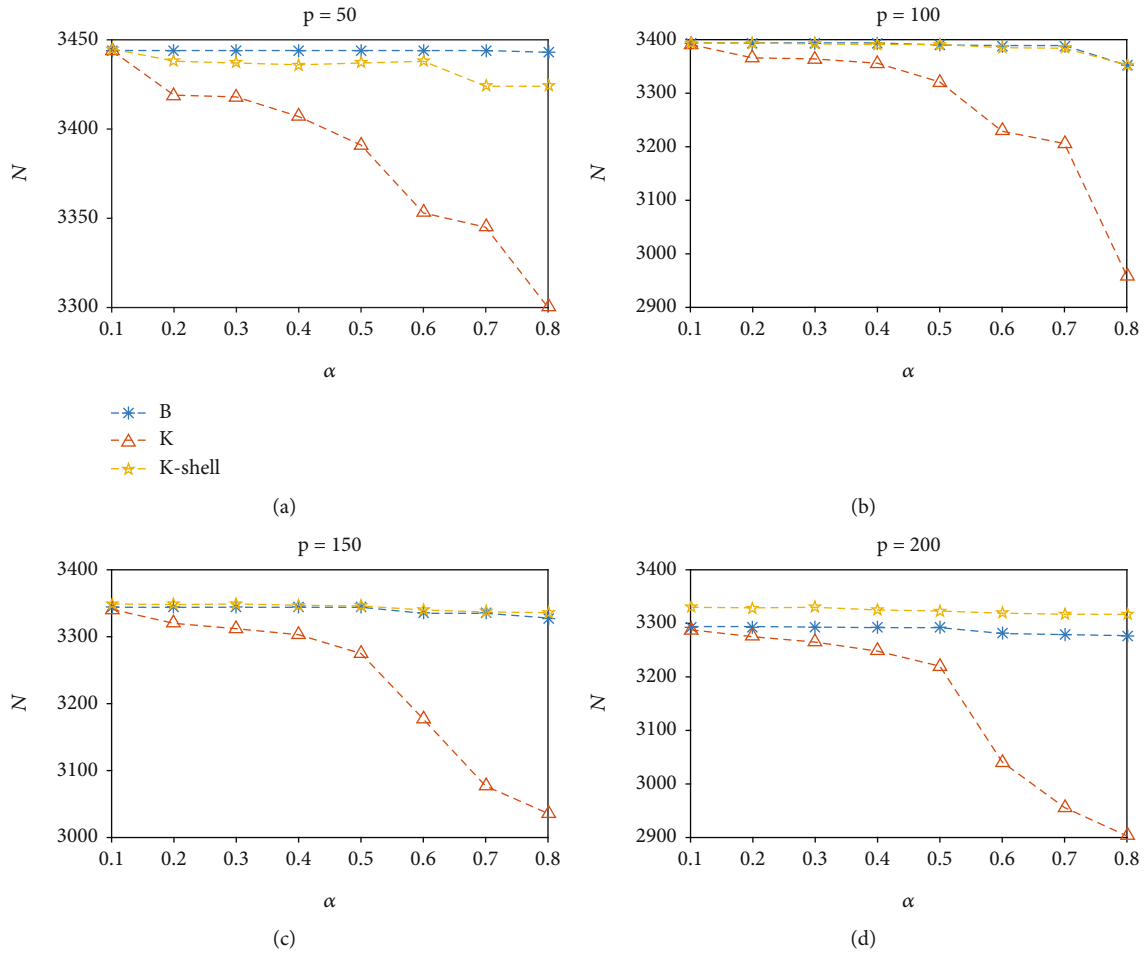


FIGURE 10: The total number of the failure nodes N (axis Y) is with different α (axis X). (a) is an image with attacking 50 nodes. (b) is an image with attacking 100 nodes. (c) is an image with attacking 150 nodes. (d) is an image with attacking 200 nodes.

regularity. Therefore, we introduce a two-dimensional graph to depict the total number of crashed nodes. In addition, we also depict time and speed accordingly.

From (a) and (b) of Figure 6, we see a strange phenomenon, and the more attacked nodes, the fewer the number of failed nodes. This is counterintuitive. However, there is a possible reason to explain this phenomenon; that is, the node that was attacked at the beginning is closely related to the nodes that are added later. The load allocated by the previous crashed node causes the subsequent node to fail. On how to answer this question, we draw a graph of the number of nodes without fail [39] (Figure 7). It turns out that for both the k -shell and the B attack, this explanation is feasible. As for how to explain the K attack, at this time, we should consider the phenomenon that the neighboring nodes fail at the same time, and the load cannot be distributed. Whether it is caused by one or both, we can conclude that, based on the previous model, increasing the number of attack nodes does not necessarily lead to an increase in network crash, especially for the B attack.

From Figures 6 and 7, we have not reached a good conclusion. However, from a time and speed perspective, we found good results. It can be seen from Figures 8 and 9 that when α is small, the speed and time of collapse reflect a better

law. As the number of attacked nodes increases, the time spent by cascade effect decreases, and the speed of collapse increases. In addition, among the three attacks, the B attack has the shortest time and the fastest speed, followed by the K attack. When α is greater than or equal to 0.6, the volatility of the data is larger, and the law is not very obvious, but it can still be seen that the B attack is more destructive to the power grid.

From this, we reasonably guess that the size of the alpha has an effect on the number of nodes that fail. To do this, we set α as the independent variable [40], set the number of failure nodes as the dependent variable, and plot the results as follows.

It can be seen from Figure 10 that as the value of α increases, the number of failure nodes decreases. But as for the B attack and the K attack, the reduction trend is not obvious. Nevertheless, some phenomena can be found from them. As you can see from Figure 10(a), that when attacking 50 nodes, no matter how large α , the number of nodes fail by the betweenness-based attack is greater than the k -shell attack. However, when the number of attacks increased, there was almost no difference in the number of failure nodes by the two modes. When the number of attacked nodes is 200, the number of failure nodes by the k -shell attack is greater

than that of the B attack. On the other hand, the number of failure nodes in the network is closely related to the load capacity of the nodes for the K attack. In this case, improving the node's performance is very effective to ensure network security.

4. Conclusions

Through the above studies, we can draw some preliminary conclusions about the cascade effect. The specific conclusions will be listed in the following points.

- (1) From the preliminary analysis, it can be roughly seen that at any time t , as the number of attacked nodes increases, so does the number of failure nodes, and the total crash time decreases
- (2) However, Figures 6 and 7 show that the increase in the number of attacked nodes does not result in an increase in the total number of crashed nodes and a decrease in the number of noncrashed nodes. Based on the data of the number of crashed and noncrashed nodes, compared with the three attack methods, B attack is affected more
- (3) Combined with the crash time and crash speed, it can be seen that the B attack has the fastest crash speed and the shortest crash time. Therefore, it can be known that in the B attack mode, the robustness of the network is the lowest, especially when α is small
- (4) Improving the load-carrying capacity of a node is a good protection measure. Judging from the results, the load-carrying capacity of nodes has more influence on the degree of network collapse than the number of attack nodes, especially in K attack
- (5) When the alpha is small, the cascading effect takes less time and is faster than the k -shell under the K attack. However, the number of failure nodes under the K attack is less than that of k -shell. Therefore, we cannot conclude that the K attack is stronger. If it is assumed that there is no way to intervene before the cascade effect stops, then the k -shell attack can be considered stronger
- (6) When α is large and there are many attacked nodes, based on our model, our conclusions above may no longer be applicable

In the above conclusions, the results have revealed the topological vulnerability of cascade in the power grid systems under different attacks and could be used to design the robust topology of wireless sensor networks [41, 42]. The understanding of the process of network collapse is conducive to better erection and use of sensor detection. Under certain measures, this is a favorable measure to deal with the network cascade effect. But for other real networks [43–48], the results are maybe different. So, we will study the vulnerability in other real-world networks with considering the community structure [49] in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

S.L., Y.C., X.W., Z.T., and X.C. declare no conflicts of interest that are directly related to the submitted work.

Authors' Contributions

Shudong Li and Yanshan Chen contributed equally to this work.

Acknowledgments

This research was funded by the Key R&D Program of Guangdong Province (No. 2019B010136003), NSFC (Nos. U1803263 and 61672020), Project of Shandong Province Higher Educational Science and Technology Program (No. J16LN61), National Key Research and Development Program of China (No. 2019QY1406), and Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019).

References

- [1] X. C. Huang, H. Qi, X. P. Zhang, L. F. Lu, and Y. Y. Hu, "Analysis on power grid vulnerability considering cascading failure of branch," *Applied Mechanics and Materials*, vol. 433-435, pp. 1254–1257, 2013.
- [2] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Electric Power Systems Research*, vol. 101, pp. 71–79, 2013.
- [3] J. Wang, C. Zhang, Y. Huang, and C. Xin, "Attack robustness of cascading model with node weight," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 37–48, 2014.
- [4] M. Ouyang, L. Zhao, Z. Pan, and L. Hong, "Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks," *Physica A: Statistical Mechanics and its Applications*, vol. 403, pp. 45–53, 2014.
- [5] Y. Yang, Z. Li, Y. Chen, X. Zhang, and S. Wang, "Improving the robustness of complex networks with preserving community structure," *PLoS One*, vol. 10, no. 2, article e0116551, 2015.
- [6] F. Tan, Y. Xia, and Z. Wei, "Robust-yet-fragile nature of interdependent networks," *Physical Review E*, vol. 91, no. 5, 2015.
- [7] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.
- [8] H.-P. Ren, J. Song, R. Yang, M. S. Baptista, and C. Grebogi, "Cascade failure analysis of power grid using new load distribution law and node removal rule," *Physica A: Statistical Mechanics and its Applications*, vol. 442, pp. 239–251, 2016.
- [9] W. Fan, S. Huang, and S. Mei, "Invulnerability of power grids based on maximum flow theory," *Physica A: Statistical Mechanics and its Applications*, vol. 462, pp. 977–985, 2016.
- [10] Y. Kornbluth, G. Barach, Y. Tuchman, B. Kadish, G. Cwilich, and S. V. Buldyrev, "Network overload due to massive attacks," *Physical Review E*, vol. 97, no. 5, 2018.

- [11] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200–210, 2017.
- [12] M. Wang, Y. Xiang, and L. Wang, "Identification of critical contingencies using solution space pruning and intelligent search," *Electric Power Systems Research*, vol. 149, pp. 220–229, 2017.
- [13] L. Shi, Q. C. Liu, J. L. Shao, and Y. Cheng, "Distributed localization in wireless sensor networks under denial-of-service attacks," *IEEE Control Systems Letters*, vol. 5, pp. 493–498, 2021.
- [14] D. Silvestre, J. P. Hespanha, and D. Silvestre, "Resilient desynchronization for decentralized medium access control," *IEEE Control Systems Letters*, vol. 5, pp. 803–808, 2020.
- [15] Y. Zheng, F. Liu, and Y.-W. Gong, "Robustness in weighted networks with cluster structure," *Mathematical Problems in Engineering*, vol. 2014, Article ID 292465, 8 pages, 2014.
- [16] X. Liu, H. Peng, and J. Gao, "Vulnerability and controllability of networks of networks," *Chaos, Solitons & Fractals*, vol. 80, pp. 125–138, 2015.
- [17] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, p. 87, 2017.
- [18] Y. Wang, G. Yan, and R. Zheng, "Vulnerability assessment of electrical cyber-physical systems against cyber attacks," *Applied Sciences*, vol. 8, no. 5, p. 768, 2018.
- [19] J. Ma and Z. Ju, "Cascading failure model of scale-free networks for avoiding edge failure," *Peer-to-Peer Networking and Applications*, vol. 12, no. 6, pp. 1627–1637, 2019.
- [20] M. I. Oozeer and S. Haykin, "Cognitive dynamic system for control and cyber-attack detection in smart grid," *IEEE Access*, vol. 7, pp. 78320–78335, 2019.
- [21] A. E. Motter, T. Nishikawa, and Y.-C. Lai, "Range-based attack on links in scale-free networks: are long-range links responsible for the small-world phenomenon?," *Physical Review E*, vol. 66, no. 6, 2002.
- [22] A. E. Motter, "Cascade Control and Defense in Complex Networks," *Physical Review Letters*, vol. 93, no. 9, 2004.
- [23] M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6266–6278, 2020.
- [24] C. Liu, H. Guo, Z. Li, X. Gao, and S. Li, "Coevolution of multi-game resolves social dilemma in network population," *Applied Mathematics and Computation*, vol. 341, pp. 402–407, 2019.
- [25] P. Zhu, X. Wang, S. Li, Y. Guo, and Z. Wang, "Investigation of epidemic spreading process on multiplex networks by incorporating fatal properties," *Applied Mathematics and Computation*, vol. 359, pp. 512–524, 2019.
- [26] M. Zheng, S. Li, D. Lu, W. Wang, X. Wu, and D. Zhao, "Structural vulnerability of power grid under malicious node-based attacks," *Communications in Computer and Information Science*, vol. 1123, pp. 446–453, 2019.
- [27] X. (. J.). du, M. Zhang, K. Nygard, S. Guizani, and H. H. Chen, "Self-healing sensor networks with distributed decision making," *International Journal of Sensor Networks*, vol. 2, no. 5/6, pp. 289–298, 2007.
- [28] S. Li, D. Zhao, X. Wu, Z. Tian, A. Li, and Z. Wang, "Functional immunization of networks based on message passing," *Applied Mathematics and Computation*, vol. 366, article 124728, 2020.
- [29] Z. Tian, C. Luo, J. Qiu, X. du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, 2020.
- [30] H. Zhang, C. Zhai, G. Xiao, and T. C. Pan, "An optimal control approach to identifying the worst-case cascading failures in power systems," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 2, pp. 956–966, 2019.
- [31] H. Zhang, C. Zhai, G. Xiao, and T. C. Pan, "Identifying critical risks of cascading failures in power systems," *IET Generation, Transmission & Distribution*, vol. 13, no. 12, pp. 2438–2445, 2019.
- [32] H. Yang, S. Li, X. Wu, H. Lu, and W. Han, "A novel solutions for malicious code detection and family clustering based on machine learning," *IEEE Access*, vol. 7, no. 1, pp. 148853–148860, 2019.
- [33] R. Yin, X. Yin, M. Cui, and Y. Xu, "Node importance evaluation method based on multi-attribute decision-making model in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, 14 pages, 2019.
- [34] Z. Yi, X. Wu, and F. Li, "Ranking spreaders in complex networks based on the most influential neighbors," *Discrete Dynamics in Nature and Society*, vol. 2018, Article ID 3649079, 6 pages, 2018.
- [35] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, 2020.
- [36] X. Du, M. Rozenblit, and M. Shayman, "Implementation and performance analysis of SNMP on a TLS/TCP base," in *2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470)*, pp. 453–466, Seattle, WA, USA, May 2001.
- [37] Y. Li, S. Li, Y. Chen, P. He, X. Wu, and W. Han, "Electric power grid invulnerability under intentional edge-based attacks," in *Dependability in Sensor, Cloud, and Big Data Systems and Applications*, vol. 1123 of Communications in Computer and Information Science, pp. 454–461, Springer, 2019.
- [38] P. Zhu, X. Wang, D. Jia, Y. Guo, S. Li, and C. Chu, "Investigating the co-evolution of node reputation and edge-strategy in prisoner's dilemma game," *Applied Mathematics and Computation*, vol. 386, p. 125474, 2020.
- [39] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3901–3909, 2020.
- [40] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *2008 IEEE International Conference on Communications*, Beijing, China, 2008.
- [41] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for Internet of Things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, Hawaii, USA, March 2018.
- [42] X. Huang and X. Du, "Achieving big data privacy via hybrid cloud," in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 512–517, Toronto, Ontario, Canada, May 2014.
- [43] D. Zhao, L. Wang, Z. Wang, and G. Xiao, "Virus propagation and patch distribution in multiplex networks: modeling,

- analysis and optimal allocation,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1755–1767, 2019.
- [44] D. Zhao, G. Xiao, Z. Wang, L. Wang, and L. Xu, “Minimum Dominating set of multiplex networks: definition, application and identification,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–15, 2020.
- [45] S. D. Li, D. N. Lu, X. B. Wu, W. Han, and D. Zhao, “Enhancing the power grid robustness against cascading failures under node-based attacks,” *Modern Physics Letters B*, vol. 35, no. 9, article 2150152, 2021.
- [46] D. Zhao, S. Yang, X. Han, S. Zhang, and Z. Wang, “Disman- tling and vertex cover of network through message passing,” *IEEE Transactions on Circuits & Systems II-Express Briefs*, vol. 67, no. 11, pp. 2732–2736, 2020.
- [47] K. Huang, Z. Wang, and M. Jusup, “Incorporating latent con- straints to enhance inference of network structure,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 466–475, 2020.
- [48] W. B. Du, X. L. Zhou, M. Jusup, and Z. Wang, “Physics of transportation: Towards optimal capacity using the multilayer network framework,” *Scientific Reports*, vol. 6, no. 1, p. 19059, 2016.
- [49] S. D. Li, L. Y. Jiang, X. B. Wu, W. H. Han, D. Zhao, and Z. Wang, “A weighted network community detection algo- rithm based on deep learning,” *Applied Mathematics and Computation*, vol. 401, no. 7, Article ID 126012, 2021.

Research Article

Research on the Evaluation Model for Wireless Sensor Network Performance Based on Mixed Multiattribute Decision-Making

Jiekun Song , Yemeng Zhang , Zhihao Zhao , and Rui Chen 

School of Economics and Management, China University of Petroleum, Qingdao 266580, China

Correspondence should be addressed to Jiekun Song; songjiekun@163.com

Received 21 March 2020; Revised 28 January 2021; Accepted 20 May 2021; Published 3 June 2021

Academic Editor: Iftikhar Ahmad

Copyright © 2021 Jiekun Song et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Many application fields initiate using wireless sensor network (WSN), and the evaluation for its performance becomes an important topic, which can help the decision-maker to find the deficiency of the current WSN or seek the best WSN. There exist mixed multiple attributes in the WSN performance evaluation process, for example, some evaluation indicators can be expressed as interval numbers, while others can be expressed as linguistic variables, so it is necessary to explore the evaluation model based on mixed multiattribute decision-making (MADM). Considering the specific evaluation purpose and requirements for different enterprises, this paper puts forward an indicator selection method and a subjective weighting method based on the rough set theory. After that, based on the transformation of mixed attributes into the unified intuitionistic fuzzy numbers (IFNs), an objective weighting method based on intuitionistic fuzzy entropy is proposed. Meanwhile, the combined weights of indicators are obtained by synthesizing the subjective and objective weights. Subsequently, in order to evaluate WSN performance objectively, an integrated comprehensive evaluation framework is proposed, which includes single evaluation, compatibility test, combination evaluation, and consistency test. The paper gives specific models and calculation steps in detail. Finally, it provides a case study to explain the application of the proposed indicator selection method and the evaluation models, which provide new ideas and references for WSN performance evaluation.

1. Introduction

WSN is a combination of multiple sensor nodes, which play a role in real-time sensing, collecting, processing, and transmitting the sensing object information. In recent years, WSN has become more and more popular in many fields, such as environmental monitoring, Internet of Things, factory maintenance, and target tracking on battlefields. In particular, enterprise production and people's life more and more rely on WSN, and how to evaluate the performance of WSN becomes more and more vital. Scientific evaluation can help decision-makers objectively compare the performance of different WSNs, so as to get the objective comparison result, improve the performance of existing WSN, or provide decision support for the selection of the best WSN. Many scholars have focused on the performance evaluation of WSN. According to the evaluation object, it mainly includes link quality [1–3], protocol performance [4–7], quality of service (QoS) [8–11], reliability [12–15], robust-

ness [16–18], and overall performance [19–23]. Gomes et al. [1] used the received signal strength indication and data packet information as indicators to test the link quality of industrial WSN. Jayasri and Hemalatha [2] put forward the link quality parameters and used Kalman filter method to evaluate the link quality. Shu et al. [3] established a link quality estimation model in terms of a support vector machine with a decision tree. Chen et al. [4] evaluated protocol performance according to coverage awareness and energy saving. Souil et al. [5] analyzed the performance of media access control (MAC) protocol using transmission probability and data delivery ratio. Mokdad et al. [6] used loss probabilities, average delay, and average delivery ratio as performance indicators to evaluate the protocol. Ketshabetswe et al. [7] compared the property of different routing protocols based on latency, success rate, energy consumption, and energy efficiency. Arora et al. [8] used throughput, end-to-end delay, network load, and other indicators to evaluate the QoS of WSN. Long et al. [9] constructed a network layer QoS

evaluation indicator system including throughput, the success rate of communication, packet loss rate, and energy efficiency. Wu et al. [10] proposed a QoS evaluation model in the basis of ideal points of vague sets. Kumar et al. [11] reviewed the machine learning techniques in QoS evaluation of WSN, including artificial neural network and reinforcement learning. He et al. [12] evaluated WSN reliability in terms of hierarchical trust rules, which combined fault evaluation with security evaluation. Zhu et al. [13] established the transmission reliability evaluation models for WSNs. Sun and Willmann [14] proposed a dependability evaluation method of industrial WSN based on deep learning. Yue and He [15] summarized the research progress of mobile WSN reliability and qualitatively analyzed different reliability schemes from packet loss rate, throughput, connectivity, and other aspects. Hu and Li [16] proposed the measurement metrics of WSN robustness, including betweenness, node degree, and connectivity coverage. Acharya and Tripathy [17] proposed four WSN cluster deployment models and compared their robustness from the first node dies, network lifetime, energy cost, and other indicators. Wang et al. [18] proposed robustness performance indicators such as power consumption, cost, and message delay and established an evaluation model based on the extension cloud theory. Jiang et al. [19] used gain-cost to represent the performance of the entire network and combined the three evaluation indicators of network efficiency, network reliability, and network connection energy cost into a function of net revenue. Zhou and Li [20] selected time delay, packet loss rate, and throughput as evaluation indicators and adopted the linear weighting method for comprehensive evaluation. Anwar et al. [21] compared trust-based security WSN and key-based security WSN from two aspects of time delay and throughput. Li et al. [22] proposed a hierarchy model from three aspects of availability, dependability, and capability and established a weighted comprehensive evaluation model for WSN performance. Luan et al. [23] summarized the performance evaluation indicators of WSN in the network layer, survivability, monitoring performance, and positioning technology and introduced a linear weighted comprehensive evaluation method. Literature review shows that the performance evaluation of WSN is actually a comprehensive process of multiple indicators. Among the evaluation methods in the existing literature, the performance indicators of WSN are mostly expressed by precise real numbers. In fact, due to the passage of time and the instability of the external environment, the values of indicators such as time delay and packet loss rate are often uncertain. In addition, the values of qualitative indicators can be expressed as linguistic variables. Therefore, based on the mixed MADM method, the establishment of a comprehensive evaluation model of WSN performance is more realistic, and the conclusion will be more scientific.

There are many ways to express the attributes of evaluation objects, which can be divided into deterministic attributes and uncertain attributes [24]. Due to the uncertainty and variability of the environment, the research on the expression and decision-making of uncertain attributes is increasingly in-depth. Zadeh [25] first proposed the concept of the fuzzy set (FS). On the basis of FS, Atanassov [26] and

Torra and Narukawa [27], respectively, introduced the intuitionistic fuzzy set (IFS) and hesitant fuzzy set (HFS) for further describing the uncertain characteristics. To associate the occurring probability of hesitant fuzzy numbers, Xu and Zhou [28] presented the probabilistic HFS. Zhu et al. [29] introduced the dual HFS as an extension of FS. Yager [30] developed the Pythagorean fuzzy set (PyFS). Cuong [31] and Smarandache [32], respectively, proposed the picture fuzzy set (PFS) and neutrosophic set as the general forms of FS and IFS. Considering that fuzzy language terms were often used for qualitative description, Zadeh [33] proposed the linguistic variable (LV) characterized by a fuzzy compatibility function. Wang and Li [34] and Rodriguez et al. [35], respectively, introduced the intuitionistic LV and the hesitant fuzzy LV. Xu [36] proposed the uncertain LV with the lower and upper limits. For comparing multiple evaluation objects, a lot of MADM methods have been developed to accommodate different attribute types. Xu and Zhao [37] reviewed the aggregation operators of IFS and proposed that some operators have ideal properties. Beliakov et al. [38] introduced the definition of the generalized aggregation of IFS, which can deal with the failure caused by the extreme value. Liu and Jin [39] developed a hybrid geometric operator of the intuitionistic uncertain LV. Besides the aggregation operator methods, some traditional methods in MADM are widely used, including distance measure [37, 39], TOPSIS (technique for order preference by similarity to ideal solution) [40], GRA (grey relational analysis) [41, 42], VIKOR (Vise Kriterijumska Optimizacija I Kompromisno Resenje) [43–45], and ER (evidence reasoning) methods [45, 46]. For the mixed MADM problem, scholars mainly put forward the distance-based methods [47–49] and the transformation technique-based methods [46, 50–55]. Lourenzutti and Krohling [48] and Pan and Geng [49], respectively, proposed a group modular random TOPSIS method and a modular random VIKOR method, which can break heterogeneous information into independent attribute modules and process information in a straight forward way without unifying. Wang and Li [50] determined the ideal alternatives and developed an interactive MADM method. Herrera et al. [51] and Liu [52] transformed the heterogeneous information into the 2-tuple LV and ranked the alternatives by dominance degree and 2-tuple linguistic weighting arithmetic average values, respectively. Bao et al. [46] aggregated the heterogeneous information into IFNs and applied integrating prospect theory and ER to rank the alternatives. Xu et al. [53] proposed an approach that aggregates the heterogeneous information into IFNs by group evaluation in rating system and TOPSIS and applied intuitionistic weighted arithmetic mean operator for ranking the alternatives. Wan et al. [54, 55] proposed an aggregation method for fusing heterogeneous information into interval-valued IFNs and applied a weighted averaging operator for ranking the alternatives. Because the transformation technique-based methods can avoid information loss to a certain extent, the research on them in mixed MADM is more extensive in recent years.

To sum up, scholars have established various WSN performance evaluation indicator systems and proposed various comprehensive evaluation models. However, the current

research needs to be deepened in the following two aspects: (1) Different evaluation subjects have different goals and requirements, so how to select evaluation indicators according to their actual situation? (2) There are both deterministic attributes and uncertain attributes in the evaluation indicator system. How to establish a more scientific comprehensive evaluation model based on the mixed MADM method? This study mainly focuses on the above two aspects, and its contributions are as follows: (1) A rough set method for WSN performance evaluation indicator selection is proposed, which can make full use of the experience of the field experts and provide relatively complete indicators that meet the needs of decision-makers. (2) An indicator weighting method based on subjective and objective synthesis is proposed, in which the subjective and objective weights of each indicator are obtained by the rough set method and by entropy technique, respectively. (3) An evaluation model based on intuitionistic fuzzy MADM is proposed, which integrates single evaluation, compatibility test, combination evaluation, and consistency test.

This article is organized as follows: Section 2 presents the indicator selection method on the basis of the rough set. Section 3 presents the indicator weighting method based on rough set and intuitionistic fuzzy entropy. Section 4 presents the evaluation model based on intuitionistic fuzzy MADM. Section 5 illustrates an example of the evaluation and selection of the WSN partner to demonstrate how to apply the proposed model. Section 6 concludes the study.

2. Indicator Selection Based on Rough Set

Due to the different evaluation purposes and requirements of WSN performance, it is difficult to establish a consistent indicator system. We design an indicator selection method based on the rough set theory to solve this problem [56, 57]. It is assumed that a comprehensive evaluation indicator system containing two levels of indicators has been preliminarily established by referring to relevant literature. The evaluation organizers investigate h experts with rich practical experience in the WSN field and invite each expert to judge the importance of t primary indicators and the corresponding secondary indicators according to the Likert's five-level scale method. The numbers from 1 to 5 represent unimportant, general, important, very important, and especially important, respectively. With each primary indicator as the decision attribute and all the corresponding secondary indicators as the condition attributes, we can get t decision tables. It shows the decision table form in Table 1, where $x_i^{(j)}$ and d_i are Likert values given by the i th expert for the importance of C_j and D relative to WSN performance evaluation.

The steps of indicator selection based on a rough set are as follows:

Step 1. According to the decision attribute D , divide the argument domains $U = \{1, 2, \dots, h\}$ into q equivalent classes: $U/D = \{H_1, H_2, \dots, H_q\}$.

TABLE 1: Decision table of a primary indicator with the corresponding secondary indicators.

Expert serial number	Condition attributes				Decision attribute
	C_1	C_2	...	C_s	D
1	$x_1^{(1)}$	$x_2^{(1)}$...	$x_s^{(1)}$	d_1
2	$x_1^{(2)}$	$x_2^{(2)}$...	$x_s^{(2)}$	d_2
...
h	$x_1^{(h)}$	$x_2^{(h)}$...	$x_s^{(h)}$	d_h

Step 2. Calculate the lower approximation of the k th equivalence class H_k regarding the conditional attribute set $C = \{C_1, C_2, \dots, C_s\}$ as follows:

$$\underline{C}H_k = \bigcup \left\{ Y \in \frac{U}{C} \right\}, k = 1, 2, \dots, q. \quad (1)$$

The C positive domain of D is as follows:

$$\text{pos}(C, D) = \bigcup_{k=1}^q \underline{C}H_k. \quad (2)$$

Step 3. Remove the attribute C_j from C , $j = 1, 2, \dots, s$ and calculate $\text{pos}(C - C_j, D)$. If $\text{pos}(C - C_j, D) = \text{pos}(C, D)$, it means that C_j is a redundant attribute and can be deleted from C . Then, we can get the reduced conditional attribute set.

Step 4. According to step 2 and step 3, continue to test whether there are redundant attributes in the reduced condition attribute set until all of the attributes are nonredundant. Then, we can get the reduced secondary indicator set C^r .

3. Indicator Weighting Based on Rough Set and Intuitionistic Fuzzy Entropy

The indicator weight has an important influence on the results of WSN performance evaluation. The subjective weight of the indicator is calculated by using the concept of relativity of rough set, so as to reflect the experts' cognition of the importance of each indicator. At the same time, the objective weight can be obtained by the intuitionistic fuzzy entropy, which can reflect the difference between the indicator values in the actual evaluation.

3.1. Indicator Weighting Based on Rough Set. Based on the reduced secondary indicators C^r , we calculate the dependence of D on C^r as follows: $\gamma(C^r, D) = |\text{pos}(C^r, D)|/|U|$, where $|\bullet|$ represents the cardinality of the set. Then, we calculate the dependence of D on the condition attribute C_j in C^r : $\sigma_{CD}(C_j) = \gamma(C^r, D) - \gamma(C^r - C_j, D)$. By standardizing $\sigma_{CD}(C_j)$ as follows:

$$w_j = \frac{\sigma_{CD}(C_j)}{\sum_{C_j \in C^r} \sigma_{CD}(C_j)}, \quad (3)$$

we can get the subjective weight of each secondary indicator relative to the primary indicator.

For a small number of primary indicators, experts can jointly determine weights based on their experience. By multiplying the weight of the secondary indicator by its corresponding weight of the primary indicator, we can obtain the composite weight of each secondary indicator. Suppose there are n secondary indicators after reduction, and their subjective weights are denoted as $\eta_j, j = 1, 2, \dots, n$.

3.2. Indicator Weighting Based on Intuitionistic Fuzzy Entropy. Because IFS take the information of membership degree, nonmembership degree, and hesitation degree into consideration at the same time, it can more accurately reflect the objective reality, and it is more reasonable for decision-makers to understand and apply. Therefore, different types of evaluation information can be uniformly transformed into IFNs, and on this basis, the weight of each attribute can be determined and the MADM can be made. references [46, 53] provided different methods to aggregate heterogeneous information into IFNs. The former is applicable to the case containing both qualitative and quantitative attributes, and the values of qualitative attributes are jointly given by group members. The latter is applicable to the case that all the attributes are qualitative, and multiple decision-makers, respectively, give the value of some attribute in the same rating system. Here, we suppose that all the attribute values of each alternative are known and refer to the former method to aggregate precise numbers, interval numbers, and linguistic variables into IFNs. Since the normalization method in [46] may produce the extreme (1, 0), making the comparison of different alternatives less objective, we suggest replacing the normalization method with vector normalization. For the triangular fuzzy numbers (TFNs) or trapezoidal fuzzy numbers (TrFNs), we can extract their cut sets and convert them to interval numbers [58]. The values of n secondary indicators of m WSNs comprise the evaluation matrix $[x_{ij}]_{m \times n}$.

Case 1. If the value of the j th indicator of each WSN is a positive precise real number, $x_{ij} > 0, i = 1, 2, \dots, m$, we can use the formula (4) to get dimensionless value y_{ij} and then convert y_{ij} to the intuitionistic fuzzy number $z_{ij} = (u_{ij}, v_{ij}) = (y_{ij}, 1 - y_{ij})$.

$$y_{ij} = \begin{cases} \frac{x_{ij}}{\sqrt{\sum_{i=1}^m x_{ij}^2}}, & c_j \in C_{\text{benefit}}, \\ \frac{1/x_{ij}}{\sqrt{\sum_{i=1}^m (1/x_{ij})^2}}, & c_j \in C_{\text{cost}}, \end{cases} \quad (4)$$

where C_{benefit} and C_{cost} represent the benefit attribute set and the cost attribute set, respectively.

Case 2. If x_{ij} is an interval number $[x_{ij}^L, x_{ij}^R], 0 < x_{ij}^L \leq x_{ij}^R, i = 1, 2, \dots, m$, we can convert it to a dimensionless interval

number $[y_{ij}^L, y_{ij}^R]$ by using the formula (5).

$$\left\{ \begin{array}{l} y_{ij}^L = \frac{x_{ij}^L}{\sqrt{\sum_{i=1}^m (x_{ij}^R)^2}}, y_{ij}^R = \begin{cases} \frac{x_{ij}^R}{\sqrt{\sum_{i=1}^m (x_{ij}^L)^2}}, \frac{x_{ij}^R}{\sqrt{\sum_{i=1}^m (x_{ij}^L)^2}} \leq 1, \\ \frac{x_{ij}^R}{\sqrt{\sum_{i=1}^m (x_{ij}^L)^2}}, \frac{x_{ij}^R}{\sqrt{\sum_{i=1}^m (x_{ij}^L)^2}} > 1, \end{cases} , c_j \in C_{\text{benefit}}, \\ y_{ij}^L = \frac{1/x_{ij}^R}{\sqrt{\sum_{i=1}^m (1/x_{ij}^L)^2}}, y_{ij}^R = \begin{cases} \frac{1/x_{ij}^L}{\sqrt{\sum_{i=1}^m (1/x_{ij}^R)^2}}, \frac{1/x_{ij}^L}{\sqrt{\sum_{i=1}^m (1/x_{ij}^R)^2}} \leq 1, \\ \frac{1/x_{ij}^L}{\sqrt{\sum_{i=1}^m (1/x_{ij}^R)^2}}, \frac{1/x_{ij}^L}{\sqrt{\sum_{i=1}^m (1/x_{ij}^R)^2}} > 1. \end{cases} , c_j \in C_{\text{cost}}. \end{array} \right. \quad (5)$$

The corresponding intuitionistic fuzzy number is $(y_{ij}^L, 1 - y_{ij}^R)$. Among them, the precise real number of x_{ij} can be first converted to an interval number $[x_{ij}, x_{ij}]$.

Case 3. If x_{ij} is a triangular fuzzy number $(x_{ij}^L, x_{ij}^M, x_{ij}^R)$ or a trapezoidal fuzzy number $(x_{ij}^L, x_{ij}^M, x_{ij}^G, x_{ij}^R)$, we can convert it to an interval number $[x_{ij}^L + (x_{ij}^M - x_{ij}^L)\alpha, x_{ij}^R - (x_{ij}^R - x_{ij}^M)\alpha]$ or $[x_{ij}^L + (x_{ij}^M - x_{ij}^L)\alpha, x_{ij}^R - (x_{ij}^R - x_{ij}^G)\alpha]$ by extracting its α -cut set and then convert the interval number to the intuitionistic fuzzy number according to the Case 2.

Case 4. If x_{ij} is an uncertain linguistic variable $[x_{ij}^{LL}, x_{ij}^{LR}]$. $x_{ij}^{LL}, x_{ij}^{LR} \in L = \{l_0, l_1, \dots, l_6\}$, $x_{ij}^{LL} < x_{ij}^{LR}$, we can quantify it to an interval number $[x_{ij}^L, x_{ij}^R]$ by the two-level proportion method (see Table 2) and convert it to the intuitionistic fuzzy number which is $(y_{ij}^L, 1 - y_{ij}^R)$ according to the Case 2. Among them, a certain linguistic variable can be first converted to an uncertain language variable $[x_{ij}, x_{ij}]$.

Entropy can reflect the degree of numerical dispersion, and the entropy method is often used for objective weighting of indicators. There are many discussions on intuitionistic fuzzy entropy [47, 59, 60]. According to the scientific axiomatic definition in reference [59], we conduct traversal simulation of various measurement formulas on the set of an intuitionistic fuzzy number $\{(u, v) \mid u \in [0, 1], v \in [0, 1 - v]\}$ and choose the formula in reference [47]. Based on the matrix $Z = [z_{ij}]_{m \times n}$, the intuitionistic fuzzy entropy of the j th indicator is as follows:

$$E_j = \frac{1}{m} \sum_{i=1}^m \frac{1 - s_{ij}^2 + 2(1 - \pi_{ij})}{2 - s_{ij}^2 + (1 - \pi_{ij})}, j = 1, 2, \dots, n, \quad (6)$$

where s_{ij} is the score of z_{ij} : $s_{ij} = u_{ij} - v_{ij}$ and π_{ij} is the accuracy of z_{ij} : $\pi_{ij} = u_{ij} + v_{ij}$.

The objective weight of the j th indicator is as follows:

$$\tau_j = \frac{1 - E_j}{\sum_{j=1}^n (1 - E_j)}, j = 1, 2, \dots, n. \quad (7)$$

TABLE 2: The corresponding of two-level proportion method.

Cost attribute	Highest	Very high	High	Average	Low	Very low	Lowest
Benefit attribute	Lowest	Very low	Low	Average	High	Very high	Highest
Quantitative value	0	1	3	5	7	9	10
Standard value	0	0.0286	0.0857	0.1429	0.2000	0.2571	0.2857

Let the weight of subjective weights be α and that of objective weights $1-\alpha$, and we can get the comprehensive weight of each indicator: $w_j = \alpha\eta_j + (1-\alpha)\tau_j, j = 1, 2, \dots, n$.

4. Evaluation Model Based on Intuitionistic Fuzzy MADM

When all the values of attributes are uniformly transformed into IFNs, WSN performance evaluation becomes an intuitionistic fuzzy MADM problem. As mentioned in the literature review, there are many intuitionistic fuzzy MADM methods. For the intuitionistic fuzzy MADM problems with known weights, the researched models mainly include aggregation operator, TOPSIS, VIKOR, GRA, and ER models. Different models have their own based-techniques and basic principles, which are summarized in Table 3. It is difficult to determine which model is most suitable for WSN performance evaluation. Each of these models is theoretically applicable. In order to fully utilize the results of various models, we put forward a combination evaluation framework that includes a single evaluation, Kendall compatibility test, combination evaluation, and Spearman consistency test.

4.1. Single Evaluation Models. Combined with the research progress of aggregation operator, TOPSIS, VIKOR, GRA, and ER models, we provide the following single performance evaluation models for WSN.

4.1.1. Aggregation Operator Model. There are a variety of forms of aggregation operators [37]. Because the HWA (hybrid weighted averaging) operator considers both the importance and the position of attributes and has such ideal properties as idempotency, boundedness, and monotony, we select HWA operator for WSN performance evaluation. The calculation steps are as follows:

Step 1. Calculate the weighted matrix: $Z' = [(z'_{ij})]_{m \times n}$, where

$$z'_{ij} = w_j(u_{ij}, v_{ij}) = (1 - (1 - u_{ij})^{w_j}, v_{ij}^{w_j}) \quad (8)$$

Step 2. Calculate the score and accuracy of z'_{ij} . In terms of the sorting rule of IFNs: (1) the higher score, the greater value; (2) when the scores are the same, the higher accuracy, the greater value, and we reorder the values of n indicators of each WSN from large to small. Let $z_{i\sigma(j)}$ be the j th intuitionistic fuzzy number, $j = 1, 2, \dots, n$, and we can get the corresponding value before weighted $z_{i\sigma(j)}$ and the indicator weight $w_{i\sigma(j)}$.

Step 3. Calculate the position weight vector by the normal distribution method. Let ω_j be the weight of the j th position; then, the comprehensive value of the i th WSN is as follows:

$$f_i = \left(1 - \prod_{j=1}^n (1 - u_{i\sigma(j)})^{w_j w_{i\sigma(j)}}, \prod_{j=1}^n (v_{i\sigma(j)})^{w_j w_{i\sigma(j)}} \right), i = 1, 2, \dots, m. \quad (9)$$

Step 4. Calculate the score and accuracy of $f_i, i = 1, 2, \dots, m$ and sort WSNs according to the sorting rule of IFNs.

4.1.2. TOPSIS Model. The basic principle of the TOPSIS model is to compare each object by its relative proximity to the ideal points. The calculation steps are as follows:

Step 1. Determine the positive and negative ideal points of evaluation matrix Z :

$$z^+ = [z_1^+, z_2^+, \dots, z_n^+], z^- = [z_1^-, z_2^-, \dots, z_n^-], \quad (10)$$

where $z_j^+ = (\max_i u_{ij}, \min_i v_{ij})$ and $z_j^- = (\min_i u_{ij}, \max_i v_{ij})$.

Step 2. Calculate the distance between the i th object and the positive and negative ideal points:

$$d_i^+ = \sum_{j=1}^n w_j d(z_{ij}, z_j^+), d_i^- = \sum_{j=1}^n w_j d(z_{ij}, z_j^-), i = 1, 2, \dots, m. \quad (11)$$

Because the distance measure in reference [47] can consider the characteristics of fluctuation and nonconcreteness of intuitionistic fuzzy information, we apply it to calculate the distance between two IFNs $z_1 = (u_1, v_1)$ and $z_2 = (u_2, v_2)$, and the formula is as follows:

$$d(z_1, z_2) = \frac{1}{6} [|u_1 - u_2| + |v_1 - v_2| + |s_1 - s_2| + (1 - \pi_1) + (1 - \pi_2)] + \frac{1}{3} \max \left(|u_1 - u_2|, |v_1 - v_2|, \frac{|\pi_1 - \pi_2|}{2} \right). \quad (12)$$

In the formula (12), s_k and π_k are the score and accuracy of z_k , respectively, $k = 1, 2$.

Step 3. Calculate the proximity of the i th WSN:

$$c_i = \frac{d_i^-}{d_i^- + d_i^+}, i = 1, 2, \dots, m. \quad (13)$$

TABLE 3: Different intuitionistic fuzzy MADM models and their principles.

Model	Based-techniques	Basic principle
Aggregation operator	Weighted integration	Intuitionistic fuzzy number after weighted aggregation
TOPSIS	Distance measure	The relative proximity from the ideal points
VIKOR	Distance measure	The trade-off between group utility and individual regret
GRA	Relational coefficient	The grey relation degree with the reference sequence
ER	Evidential reasoning algorithms, distance measure	The belief degree relative to the ideal points

Sort all the WSNs according to their proximities from large to small.

4.1.3. VIKOR Model. VIKOR model takes both group utility and individual regret into account, and it can reflect the preference of decision-makers by the trade-off coefficient. Firstly, calculate the group utility value P_i and the individual regret value N_i of the i th WSN:

$$P_i = \sum_{j=1}^n \frac{w_j d(z_{ij}, z_j^+)}{d(z_j^-, z_j^+)}, i = 1, 2, \dots, m, \quad (14)$$

$$N_i = \max_j \frac{w_j d(z_{ij}, z_j^+)}{d(z_j^-, z_j^+)}, i = 1, 2, \dots, m.$$

Secondly, calculate the benefit ratio value Q_i :

$$Q_i = \frac{\gamma(P_i - \min_k P_k)}{\max_k P_k - \min_k P_k} + \frac{(1 - \gamma)(N_i - \min_k N_k)}{\max_k N_k - \min_k N_k}, i = 1, 2, \dots, m, \quad (15)$$

where γ is the trade-off coefficient between the group utility and individual regret, $0 \leq \gamma \leq 1$.

Finally, sort all the WSNs according to their benefit ratio values from small to large.

4.1.4. GRA Model. The principle of GRA is to evaluate each object according to its relation degree with the reference sequence (usually positive ideal point). Firstly, calculate the relation coefficient between the j th indicator of the i th WSN and the positive ideal point:

$$\xi_{ij} = \frac{\min_j \min_d(z_{ij}, z_j^+) + \rho \max_i \max_d(z_{ij}, z_j^+)}{d(z_{ij}, z_j^+) + \rho \max_i \max_d(z_{ij}, z_j^+)}, i = 1, 2, \dots, m; j = 1, 2, \dots, n, \quad (16)$$

where ρ is the distinguishing coefficient, $\rho \in [0, 1]$.

Secondly, calculate the relation degree of the i th WSN:

$$\xi_i = \sum_{j=1}^n w_j \xi_{ij}, i = 1, 2, \dots, m. \quad (17)$$

Finally, sort all the WSNs according to their relation degrees from large to small.

4.1.5. ER Model. Each indicator of the evaluation object in the ER model is regarded as proof. Based on the identification framework composed of multiple evaluation grades, we can evaluate each proof and get the belief degree that it belongs to each grade. By combining the weight of each indicator, we can use the evidence of reasoning algorithm to get the belief degree of the evaluation object. In this paper, we use the IDS software for the evidence of reasoning of WSN performance [61], and the steps are as follows:

Step 1. Build an indicator hierarchy comprising a top attribute and n bottom attributes. The top attribute has the best and the worst grade, and the utility values are 1 and 0, respectively. The bottom attributes also have the best and the worst grade, and the belief degree vectors of them for the combination (best, worst) are (1, 0) and (0, 1), respectively. Input the weights of n bottom attributes into the IDS software.

Step 2. Insert m alternatives and input the belief degree that the j th indicator of the i th alternative belongs to the best and worst grades, that is, the value expressed in the form of an intuitionistic fuzzy number (u_{ij}, v_{ij}) .

Step 3. Evaluate the i th alternative and get the belief degree vector of the top attribute for the combination (best, worst), namely, the intuitionistic fuzzy number $e_i = (u_i, v_i)$, $i = 1, 2, \dots, m$.

Step 4. Calculate the score and accuracy of e_i and sort all the WSNs according to the sorting rule of an intuitionistic fuzzy number.

4.2. Kendall Compatibility Test. Since the evaluation results of the above single models may differ greatly, we need to obtain less divergent evaluation results through compatibility test, so as to conduct further combination evaluation [62]. Let r_{ik} be the rank of the i th WSN in the k th single model, $i = 1, 2, \dots, n$; $k = 1, 2, \dots, g$. When $n \leq 7$, we can calculate Kendall's coefficient of concordance as follows:

$$s = \sum_{i=1}^n r_i^2 - \frac{1}{n} \left(\sum_{i=1}^n r_i \right)^2 = \sum_{i=1}^n \left(\sum_{k=1}^g r_{ik} \right)^2 - \frac{1}{n} \left(\sum_{i=1}^n \sum_{k=1}^g r_{ik} \right)^2. \quad (18)$$

Given the significance level α , if the value s is no less than the critical value $s_\alpha(g, n)$, then the g models are compatible.

When $n > 7$, we calculate the statistical indicator: $\chi^2 = g(n-1)W$, where

$$W = \frac{12 \sum_{i=1}^n r_i^2}{g^2 n(n^2 - 1)} - \frac{3(n+1)}{n-1}. \quad (19)$$

Given the significance level α , if the value χ^2 is no less than the critical value $\chi^2_\alpha(n-1)$, then the g models are compatible.

For the case of incompatibility, we can calculate the statistical indicator of the remaining models by eliminating a single model and obtain the set of compatible models with the largest statistical value.

4.3. Combination Evaluation Models. The evaluation values of each WSN in the above single models are all in the range $[-1, 1]$, and their meanings are clear. In order to fully utilize of the evaluation information, we further carry out the combination evaluation according to the numerical value rather than ranking. To eliminate the influence of actual value range difference between models and keep the correlation of the previous results unchanged, we firstly apply the extremum transformational method to convert the original results into the range $[0, 1]$. Among them, the benefit ratio value in the VIKOR model is converted according to the conversion method of the cost indicator, and the results of the other four models are converted according to the conversion method of the benefit indicator. Let t_{ik} be the result from the i th WSN in the k th compatible model after the extremum transformation, $i = 1, 2, \dots, m, k = 1, 2, \dots, g$. The widely used combination evaluation models based on the numerical value mainly include averaging, principal component analysis (PCA), MSE- (mean square error-) based weighted, optimization, drift, and cooperative game models [63, 64]. Since the PCA model requires a large number of samples, we apply the other five models for combination evaluation.

4.3.1. Averaging Model. All the single evaluation models have the same status in this combination model, and the average value of the results in g compatible models for each WSN is its combination evaluation result.

4.3.2. MSE-Based Weighted Model. This model is an objective weighted method. By calculating the MSE of the k th compatible model and taking its proportion to the MSEs' sum of all the g models as the weight w_k , we can calculate the combination evaluation result of each WSN as follows:

$$t_i = \sum_{k=1}^g w_k t_{ik}, \quad i = 1, 2, \dots, m. \quad (20)$$

4.3.3. Optimization Model. The objective function is to minimize the sum of the error squares between the weighted combination results and the single evaluation results of all WSNs. We can get the optimal weights of all the compatible models by solving the optimization model and can calculate

the combination evaluation result by substituting them into formula (20).

4.3.4. Drift Model. Assuming there exists an objective model, the weight of each model can be calculated based on the drift of its result relative to the result of the objective model. The further the drift, the greater the weight. In this paper, we assume that the averaging model, MSE-weighted model, or optimization model is the objective model and record its evaluation result as the reference $r = [r_1, r_2, \dots, r_m]$. Calculate the correlation coefficient c_k between the result of the k th single evaluation model and the reference [65], then the drift is $p_k = 1 - c_k$, and the weight is as follows:

$$w_k = \frac{\max_l p_l + \min_l p_l - p_k}{\sum_{k=1}^g (\max_l p_l + \min_l p_l - p_k)}, \quad k = 1, 2, \dots, g. \quad (21)$$

Substitute the weights of all the single evaluation models into the formula (20), and we can get the combination evaluation result.

4.3.5. Cooperative Game Model. Assuming there exists an objective model, we calculate the average absolute error between the result of the k th single evaluation model and that of the objective model as the characteristic function of the alliance $\{k\}$:

$$v(\{k\}) = \frac{\sum_{i=1}^m |t_{ik} - r_i|}{m}, \quad k = 1, 2, \dots, g. \quad (22)$$

Similarly, we can calculate the characteristic functions of the $2^g - 2$ alliances. Let $v(S) - v(S \setminus \{k\})$ be the contribution of the k th model to alliance S , and then, we can get the Shapley value ϕ_k of the k th model as its average contribution to the whole alliance $\Omega = \{1, 2, \dots, g\}$:

$$\phi_k = \sum_{S \subset \Omega} \frac{(g - |S|)! (|S| - 1)!}{g!} [v(S) - v(S \setminus \{k\})], \quad k = 1, 2, \dots, g. \quad (23)$$

The weight of the k th model is as follows:

$$w_k = \frac{1}{g-1} \cdot \frac{v(\Omega) - \phi_k}{v(\Omega)}, \quad k = 1, 2, \dots, g. \quad (24)$$

Substitute the weights of all the single evaluation models into the formula (20), and then, we can get the combination evaluation result.

4.4. Spearman Consistency Test. The method of Spearman rank correlation coefficient can be used to test the consistency between each combination evaluation model and all the compatible model set [63, 64]. The Spearman rank correlation coefficient between the l th combination model and the

k th single evaluation model is as follows:

$$\rho_{lk} = 1 - \frac{6 \sum_{i=1}^n (p_{il} - p_{ik})^2}{n(n^2 - 1)}, \quad (25)$$

where p_{il} and p_{ik} are the ranks of the i th WSN in the l th combination evaluation model and the k th single evaluation model, respectively, $i = 1, 2, \dots, n$; $l = 1, 2, \dots, 9$; $k = 1, 2, \dots, g$.

When $n < 10$, we calculate the average correlation coefficient as follows:

$$\rho_l = \frac{1}{g} \sum_{k=1}^g \rho_{lk}, \quad l = 1, 2, \dots, 9. \quad (26)$$

Then, we output the ranking result in the combination model with the maximum average correlation coefficient as the ultimate evaluation result.

When $n \geq 10$, we can calculate the statistical indicator as follows:

$$t_l = \rho_l \sqrt{\frac{n-2}{1-\rho_l^2}}, \quad l = 1, 2, \dots, 9. \quad (27)$$

Given the significance level α , if the value t_l is no less than the critical value $t_\alpha(n-2)$, it means that the l th combination evaluation model is consistent with the compatible model set. Then, we output the ranking result of the combination model with the largest statistical value and passed the consistency test as the final evaluation result.

5. A Case Study

The decision-makers of company H, a manufacturer of cold chain products, plan to choose the best WSN partner for the Internet of Things from five WSNs: A_1, A_2, \dots, A_5 . The preliminary evaluation indicator system is shown in Figure 1.

Considering the possibility of redundancy between indicators, we use the proposed rough set method to select indicators. Taking the network layer QoS as an example, we get the decision table by consulting ten experts in Table 4. For example, the first expert thinks that the packet loss rate is especially important for the network layer QoS, and network layer QoS is important for the WSN performance evaluation, so the Likert value for the importance of the packet loss rate is 5, and that of the network layer QoS is 3. Following the reduction steps, we get five reduction sets of conditional attributes that include {energy consumption balance, time delay}, {energy consumption balance, time delay jitter}, {packet loss rate, energy consumption balance, time delay jitter}, {energy efficiency, energy consumption balance, time delay jitter}, and {packet loss rate, throughput, energy efficiency, time delay}. Through further consultation with experts, we select the four elements in the fifth reduction set as the secondary indicators.

Similarly, we get the secondary indicators of reliability including security, survivability, and anti-interference capability and those of monitoring performance including network coverage, self-organizing ability, and sensor node capability. According to formula (3), we calculate the weight of each secondary indicator relative to the primary indicator. The experts consider that each primary indicator has the same weight 1/3; then, we can get the weight of each indicator for WSN performance evaluation in Table 5.

Through expert interviews and data monitoring, we get the original evaluation data of five alternative WSN partners in Table 6. The indicators C_1, C_2, C_3 , and C_4 are expressed as interval numbers, C_8 is expressed as a precise real number, and the other five indicators are expressed linguistic variables from the seven-level linguistic term set {highest, very high, high, average, low, very low, lowest}.

After vector normalization of the above evaluation matrix elements and the unified conversion to IFNs, we get the intuitionistic fuzzy decision-making matrix as follows:

$$Z' = \begin{bmatrix} (0.2911, 0.5602) & (0.2815, 0.3716) & (0.2657, 0.3874) & (0.2944, 0.3549) & (0.4276, 0.2230) \\ (0.2289, 0.4938) & (0.3614, 0.3921) & (0.3561, 0.3035) & (0.3429, 0.3524) & (0.3296, 0.4210) \\ (0.3569, 0.4611) & (0.3500, 0.4970) & (0.3714, 0.4044) & (0.4045, 0.3713) & (0.3085, 0.4970) \\ (0.3465, 0.4768) & (0.3879, 0.3851) & (0.3690, 0.4308) & (0.3730, 0.4458) & (0.3330, 0.5102) \\ (0.3819, 0.3016) & (0.2728, 0.5111) & (0.4910, 0.3714) & (0.2728, 0.6508) & (0.2728, 0.3714) \\ (0.3095, 0.6010) & (0.4333, 0.4413) & (0.3095, 0.2817) & (0.1857, 0.6010) & (0.4333, 0.2817) \\ (0.3304, 0.4413) & (0.3304, 0.6010) & (0.1982, 0.6010) & (0.4626, 0.2817) & (0.4626, 0.4413) \\ (0.4428, 0.5572) & (0.4644, 0.5356) & (0.4428, 0.5572) & (0.4320, 0.5680) & (0.4536, 0.5464) \\ (0.3304, 0.4413) & (0.3304, 0.6010) & (0.4626, 0.2817) & (0.1982, 0.6010) & (0.4626, 0.4413) \\ (0.2182, 0.5377) & (0.5092, 0.1679) & (0.3637, 0.5377) & (0.3637, 0.3528) & (0.2182, 0.7226) \end{bmatrix}. \quad (28)$$

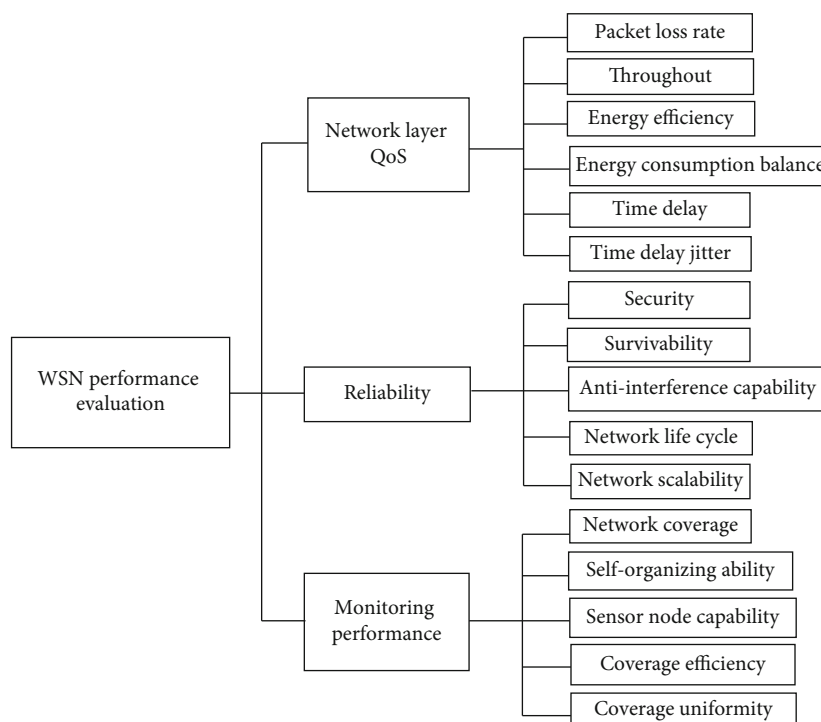


FIGURE 1: The preliminary evaluation indicator system.

TABLE 4: The decision table of the network layer QoS.

Expert serial number	Packet loss rate	Throughput	Energy efficiency	Energy consumption balance	Time delay	Time delay jitter	Network layer QoS
1	5	5	3	5	4	2	3
2	4	5	4	5	5	3	5
3	5	4	4	4	4	3	4
4	4	5	3	4	5	2	3
5	4	4	4	4	4	4	4
6	4	4	3	5	5	3	5
7	5	5	4	5	4	2	3
8	4	5	4	4	4	3	4
9	4	4	3	5	4	2	3
10	5	4	5	3	5	3	4

According to formulas (6) and (7), the intuitionistic fuzzy entropy weights of ten indicators are 0.0811, 0.0839, 0.0979, 0.0990, 0.0964, 0.0962, 0.1047, 0.1335, 0.1047, and 0.1025 in sequence. Suppose the weights of the subjective and objective weights are both 0.5, the combination weights of ten indicators are 0.0644, 0.0896, 0.0966, 0.0971, 0.0853, 0.1222, 0.1079, 0.1052, 0.1036, and 0.1282 in sequence. By using the aggregation operator, TOPSIS, VIKOR, GRA, and ER models, we get their evaluation results as shown in Table 7.

The results of these five single models are not consistent. In particular, the result of the VIKOR model is significantly different from those of the other four models, which may be caused by the fact that the VIKOR model considers individual regret factor at the same time. Kendall’s coefficient of concordance equals 110, which is less than the critical value

$s_{0.05}(5, 5) = 112.3$, so the five single evaluation models are not compatible. By removing a single model at a time, we get the statistical value of the remaining models as shown in Table 8.

Remove the VIKOR model, and Kendall’s coefficient of concordance of the other four models equals 106, greater than the critical value $s_{0.05}(5, 4) = 88.4$, so the remaining four models are compatible. By applying the extremum transformation method, we convert the results of four single evaluation models into the range $[0, 1]$. By substituting the normalized values into the averaging, MSE-based weighted, and optimization combination models, we find that the optimal weights of four compatible models are all 0.25, indicating that the result of the optimization model is the same as that of the averaging model. Taking the averaging and MES-based

TABLE 5: The weights of indicators for WSN performance evaluation.

Primary indicator	Secondary indicator		Composite weight
	Name	Implication	
Network layer QoS (1/3)	Packet loss rate, C_1 (0.1429)	The number of packets lost during information transmission	0.0476
	Throughput, C_2 (0.2857)	Total data volume between gateway node and sensor nodes in the monitoring area	0.0952
	Energy efficiency, C_3 (0.2857)	The ratio of total energy consumption to throughput	0.0952
	Time delay, C_4 (0.2857)	Time difference between the first packet and the last packet to the gateway node	0.0952
Reliability (1/3)	Security, C_5 (0.2222)	The ability of the network to guarantee the availability, confidentiality, authenticity, and integrity of the information	0.0741
	Survivability, C_6 (0.4444)	The ability of the network node to maintain its function under the condition of natural failure or intentional attack	0.1481
	Anti-interference capability, C_7 (0.3333)	The ability of the network to resist the interference of adversary by electromagnetic energy and nonadversary	0.1111
Monitoring performance (1/3)	Network coverage, C_8 (0.2308)	Coverage of sensor nodes to the target monitoring area in WSN	0.0769
	Self-organizing ability, C_9 (0.3077)	The ability of network nodes to determine their location and dynamically configure and manage themselves after deployment	0.1026
	Sensor node capability, C_{10} (0.4615)	The ability of sensor nodes to collect raw data, process local information, communicate wirelessly, route and forward, and work together with other nodes	0.1538

Note: the value in brackets is the weight of the indicator relative to the upper-level indicator.

TABLE 6: The original evaluation data.

Indicator	A_1	A_2	A_3	A_4	A_5
C_1	[0.2825,0.3030]	[0.1977,0.3134]	[0.2028,0.3320]	[0.1926,0.2996]	[0.1599,0.2063]
C_2	[1245,2016]	[1966,2421]	[1937,2774]	[1865,2579]	[1793,2306]
C_3	[0.42,0.51]	[0.45,0.52]	[0.38,0.49]	[0.36,0.45]	[0.45,0.59]
C_4	[0.0161,0.0197]	[0.0137,0.0176]	[0.0148,0.0185]	[0.0152,0.0183]	[0.0172,0.0205]
C_5	[high, highest]	[average, high]	Very high	Average	[average, very high]
C_6	Average	High	[average, very high]	[low, average]	[high, very high]
C_7	[average, high]	Average	[low, average]	[high, very high]	High
C_8	82%	86%	82%	80%	84%
C_9	[average, high]	Average	[high, very high]	[low, average]	High
C_{10}	[low, average]	[high, very high]	Average	[average, high]	Low

TABLE 7: The results of single evaluation models.

WSN	Aggregation operator		TOPSIS		VIKOR		GRA		ER	
	Comprehensive value	Rank	Proximity	Rank	Benefit ratio value	Rank	Relation degree	Rank	Belief degree	Rank
A_1	(0.3281,0.4954)	5	0.5026	5	0.8333	3	0.8979	5	(0.3214,0.5342)	5
A_2	(0.3805,0.4539)	3	0.5268	1	0.0000	1	0.9210	2	(0.3926,0.4745)	2
A_3	(0.3825,0.4162)	1	0.5253	2	0.3974	5	0.9228	3	(0.3785,0.4525)	1
A_4	(0.3425,0.4469)	4	0.5122	4	0.8687	2	0.9094	1	(0.3392,0.4998)	4
A_5	(0.3805,0.4312)	2	0.5138	3	0.4424	4	0.9100	4	(0.3758,0.4913)	3

TABLE 8: The statistical value of the remaining models by removing a single model.

The removed model	Kendall's coefficient of concordance
Aggregation operator	78
TOPSIS	58
VIKOR	106
GRA	74
ER	64

TABLE 9: The results of combination evaluation models.

WSN	Averaging	MSE-based	Drift		Cooperative game	
			Averaging	MSE-based	Averaging	MSE-based
A_1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
A_2	0.8932	0.8955	0.9470	0.9474	0.9186	0.9198
A_3	0.9844	0.9842	0.9834	0.9832	0.9859	0.9858
A_4	0.4254	0.4245	0.4107	0.4108	0.4188	0.4186
A_5	0.6300	0.6280	0.5722	0.5710	0.6042	0.6024

weighted models as the objective model, we get the results of the drift and cooperative game models. The results of six combination evaluation models are summarized in Table 9.

The ranking results of six combination evaluation models are identical, i.e., $A_3 > A_2 > A_5 > A_4 > A_1 > A_6$. The average correlation coefficient is 0.775, indicating that the results of the combination evaluation models have great consistency with the single evaluation models. It can be seen that the combination evaluation can make full use of the evaluation information, overcome the shortcomings, and retain the advantages of each method, so as to realize the consistent fusion of different single evaluation models. According to the above ranking results, company H can give priority to A_3 as the WSN partner.

6. Conclusions

In this research, considering that the purposes and requirements of different enterprises for WSN performance evaluation are not the same, we propose a method of indicator selection based on the rough set. By consulting experts with Likert's five-level scale and using the attribute reduction method of the rough set, we can obtain a relatively small-scale WSN performance evaluation indicator system that reflects the individual experience and judgment of experts. In addition, based on the decision tables, we also calculate the subjective weights of indicators by using the concept of dependence.

Considering the mixed multiattribute characteristics of the indicators, we first transform the precise real numbers, interval numbers, linguistic variables, TFNs, and TrFNs into the unified form of IFNs. Then, we calculate the objective weights of indicators on the basis of intuitionistic fuzzy entropy. By the linear combination of subjective and objective weights, we get the comprehensive weights.

Based on the research progress of intuitionistic fuzzy MADM methods, we put forward five single evaluation models for WSN performance, including aggregation operator, TOPSIS, VIKOR, GRA, and ER models. In order to make full use of their results, we propose the thought and framework of combination evaluation. First, we perform the Kendall compatibility test to get the compatible model set. Second, we apply the averaging, MSE-based weighted, optimization, drift, and cooperative game models to perform the combination evaluation. Third, we carry out the Spearman consistency test to get the best combination evaluation result.

The case study proves that the proposed indicator selection method and the evaluation models are feasible and efficient. In practice, decision-makers can apply the thought and method in this paper for performance evaluation or optimal selection of WSN.

Even though this study considers the mangle multiple attributes in the WSN performance evaluation process, there still exist other expression forms of evaluation indicators that should be taken into consideration. For instance, the values of indicators may contain the other forms, such as hesitant fuzzy number, Pythagorean fuzzy number, picture fuzzy number, and spherical fuzzy number simultaneously, so finding the way of unifying them into a consistent form with little information distortion is necessary for the future. The rough set method is used for subjective weight determination in this study. Actually, in addition to this method, there exist other methods suitable for subjective indicator weighting. For instance, the analytic network process (ANP) can take the correlations among indicators at the same level into consideration. Therefore, integrating the rough set method and other subjective weighting methods to improve indicator weighting may also be another future research direction.

Data Availability

The gathered data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (71871222).

References

- [1] R. D. Gomes, D. V. Queiroz, A. C. Lima Filho, I. E. Fonseca, and M. S. Alencar, "Real-time link quality estimation for industrial wireless sensor networks using dedicated nodes," *Ad Hoc Networks*, vol. 59, pp. 116–133, 2017.
- [2] T. Jayasri and M. Hemalatha, "Link quality estimation for adaptive data streaming in WSN," *Wireless Pers Commun*, vol. 94, no. 3, pp. 1543–1562, 2017.
- [3] J. Shu, S. Liu, L. Liu, L. Zhan, and G. Hu, "Research on link quality estimation mechanism for wireless sensor networks

- based on support vector machine,” *Chinese Journal of Electronics*, vol. 26, no. 2, pp. 377–384, 2017.
- [4] D. Chen, L. Chen, M. Chen, and M. Y. Hsu, “A coverage-aware and energy-efficient protocol for the distributed wireless sensor networks,” *Computer Communications*, vol. 137, pp. 15–31, 2019.
- [5] M. Souil, A. Bouabdallah, and A. E. Kamal, “Efficient QoS provisioning at the MAC layer in heterogeneous wireless sensor networks,” *Computer Communications*, vol. 43, pp. 16–30, 2014.
- [6] L. Mokdad, J. Ben-Othman, B. Yahya, and S. Niagne, “Performance evaluation tools for QoS MAC protocol for wireless sensor networks,” *Ad Hoc Networks*, vol. 12, pp. 86–99, 2014.
- [7] L. K. Ketshebetswe, A. U. M. Zungeru, M. Mangwala, J. M. Chuma, and B. Sigweni, “Communication protocols for wireless sensor networks: a survey and comparison,” *Heliyon*, vol. 5, no. 5, article e01591, 2019.
- [8] V. K. Arora, V. Sharma, and M. Sachdeva, “On QoS evaluation for ZigBee incorporated wireless sensor network (IEEE 802.15.4) using mobile sensor nodes,” *Journal of King Saud University – Computer and Information Sciences*, 2018.
- [9] Y. Long, Y. Wu, X. Wang, R. Feng, and J. Wan, “Research on evaluation method for network layer QoS in wireless sensor networks,” *Chinese Journal of Sensors and Actuators*, vol. 23, no. 12, pp. 1766–1771, 2010.
- [10] J. Wu, L. Wang, and H. Shi, “Method to evaluate WNS QoS,” *Journal of Hainan Tropical Ocean University*, vol. 25, no. 5, pp. 80–85, 2018.
- [11] D. Praveen Kumar, T. Amgoth, and C. S. R. Annavarapu, “Machine learning algorithms for wireless sensor networks: a survey,” *Information Fusion*, vol. 49, pp. 1–25, 2019.
- [12] W. He, G. Hu, Z. Zhou et al., “A new hierarchical belief-rule-based method for reliability evaluation of wireless sensor network,” *Microelectronics Reliability*, vol. 87, pp. 33–51, 2018.
- [13] X. Zhu, Y. Lu, J. Han, and L. Shi, “Transmission reliability evaluation for wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 2.
- [14] D. Sun and S. Willmann, “Deep learning-based dependability assessment method for industrial wireless network,” *IFAC PapersOnLine*, vol. 52, pp. 219–224, 2019.
- [15] Y. Yue and P. He, “A comprehensive survey on the reliability of mobile wireless sensor networks: taxonomy, challenges, and future directions,” *Information Fusion*, vol. 44, pp. 188–204, 2018.
- [16] S. Hu and J. Li, “TMSE: a topology modification strategy to enhance the robustness of scale-free wireless sensor networks,” *Computer Communications*, vol. 157, pp. 53–63, 2020.
- [17] S. Acharya and C. R. Tripathy, “A reliable fault-tolerant ANFIS model based data aggregation scheme for Wireless Sensor Networks,” *Journal of King Saud University – Computer and Information Sciences*, vol. 32, no. 6, pp. 741–753, 2020.
- [18] Z. Wang, D. Wang, Q. Zhang, and Z. Zhang, “Robustness evaluation of WSN based on extension cloud theory,” *Software Guide*, vol. 16, no. 7, pp. 1–4, 2017.
- [19] N. Jiang, B. Li, P. Pan, T. Wan, and L. Liu, “C-POEM: comprehensive performance optimization evaluation model for wireless sensor networks,” *Soft Computing*, vol. 21, no. 12, pp. 3377–3385, 2017.
- [20] C. Zhou and X. Li, “Research on comprehensive evaluation of industrial wireless sensor network performance,” *Computer Engineering*, vol. 36, no. 16, pp. 82–84, 2010.
- [21] R. W. Anwar, A. Zainal, F. Outay, A. Yasar, and S. Iqbal, “BTEM: belief based trust evaluation mechanism for wireless sensor networks,” *Future Generation Computer Systems*, vol. 96, pp. 605–616, 2019.
- [22] G. Li, W. Jiang, and J. Tao, “Effectiveness evaluation of wireless sensor networks based on AHP,” *Informatization Research*, vol. 43, no. 6, pp. 74–78, 2017.
- [23] J. Luan, Q. Wang, X. He et al., “Analysis of wireless sensor network performance evaluation,” *Machine Building Automation*, vol. 44, no. 3, pp. 165–167, 2015.
- [24] J. F. Pang and J. Y. Liang, “Evaluation of the results of multi-attribute group decision-making with linguistic information,” *Omega*, vol. 40, no. 3, pp. 294–301, 2012.
- [25] L. A. Zadeh, “Fuzzy sets,” *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.
- [26] K. Atanassov, “Intuitionistic fuzzy sets,” *Fuzzy Sets and Systems*, vol. 20, no. 1, pp. 87–96, 1986.
- [27] V. Torra and Y. Narukawa, “On hesitant fuzzy sets and decision,” in *2009 IEEE International Conference on Fuzzy Systems*, pp. 1378–1382, Jeju Island, Korea, August 2009.
- [28] Z. Xu and W. Zhou, “Consensus building with a group of decision makers under the hesitant probabilistic fuzzy environment,” *Fuzzy Optimization and Decision Making*, vol. 16, no. 4, pp. 481–503, 2017.
- [29] B. Zhu, Z. Xu, and M. Xia, “Dual hesitant fuzzy sets,” *Journal of Applied Mathematics*, vol. 2012, Article ID 879629, 13 pages, 2012.
- [30] R. R. Yager, “Pythagorean fuzzy subsets,” in *2013 Joint IFSA World Congress and NAFIPS Annual Meeting (IFSA/NAFIPS)*, pp. 57–61, Edmonton, Canada, June 2013.
- [31] B. C. Cuong, “Picture fuzzy sets,” *Journal of Computer Science and Cybernetics*, vol. 30, no. 4, pp. 409–420, 2014.
- [32] F. Smarandache, *A Unifying Field in Logics: Neutrosophic Logic*, Am. Res. Press, Rehoboth, 1999.
- [33] L. A. Zadeh, “The concept of a linguistic variable and its application to approximate reasoning: part III,” *Information Sciences*, vol. 9, no. 1, pp. 43–80, 1975.
- [34] J. Q. Wang and J. J. Li, “The multi-criteria group decision making method based on multi-granularity intuitionistic two semantics,” *Science & Technology Information*, vol. 33, pp. 8–9, 2009.
- [35] R. M. Rodriguez, L. Martinez, and F. Herrera, “Hesitant fuzzy linguistic term sets for decision making,” *IEEE Transactions on Fuzzy Systems*, vol. 20, no. 1, pp. 109–119, 2012.
- [36] Z. S. Xu, “Induced uncertain linguistic OWA operators applied to group decision making,” *Information Fusion*, vol. 7, no. 2, pp. 231–238, 2006.
- [37] Z. Xu and N. Zhao, “Information fusion for intuitionistic fuzzy decision making: an overview,” *Information Fusion*, vol. 28, pp. 10–23, 2016.
- [38] G. Beliakov, H. Bustince, D. P. Goswami, U. K. Mukherjee, and N. R. Pal, “On averaging operators for Atanassov’s intuitionistic fuzzy sets,” *Information Sciences*, vol. 181, no. 6, pp. 1116–1124, 2011.
- [39] P. Liu and F. Jin, “Methods for aggregating intuitionistic uncertain linguistic variables and their application to group decision making,” *Information Sciences*, vol. 205, pp. 58–71, 2012.
- [40] S. Zeng, A. Hussain, T. Mahmood, M. Irfan Ali, S. Ashraf, and M. Munir, “Covering-based spherical fuzzy rough set model

- hybrid with TOPSIS for multi-attribute decision-making,” *Symmetry*, vol. 11, no. 4, p. 547, 2019.
- [41] W. L. Liu and P. D. Liu, “Hybrid multiple attribute decision making method based on relative approach degree of grey relation projection,” *African Journal of Business Management*, vol. 4, no. 17, pp. 3716–3724, 2010.
- [42] G. W. Wei, “GRA method for multiple attribute decision making with incomplete weight information in intuitionistic fuzzy setting,” *Knowledge-Based Systems*, vol. 23, no. 3, pp. 243–247, 2010.
- [43] J. H. Park, H. J. Cho, and Y. C. Kwun, “Extension of the VIKOR method to dynamic intuitionistic fuzzy multiple attribute decision making,” *Computers and Mathematics with Applications*, vol. 65, no. 4, pp. 731–744, 2013.
- [44] S. Opricovic and G. H. Tzeng, “Extended VIKOR method in comparison with outranking methods,” *European Journal of Operational Research*, vol. 178, no. 2, pp. 514–529, 2007.
- [45] R. Wang, W. Li, X. Luo, and C. Lv, “Extended VIKOR method of multi-attribute decision making under intuitionistic fuzzy environment based on a new distance measure,” *Systems Engineering and Electronics*, vol. 41, no. 11, pp. 2524–2532, 2019.
- [46] T. Bao, X. Xie, and P. Meng, “Intuitionistic fuzzy hybrid multi-criteria decision making based on prospect theory and evidential reasoning,” *System Engineering—Theory and Practice*, vol. 37, no. 2, pp. 460–468, 2017.
- [47] Y. Li, Y. Chen, C. Luo, and Z. Cai, “Method for multi-attribute decision making based on probabilistic hesitant-intuitionistic fuzzy entropy and evidential reasoning,” *Systems Engineering and Electronics*, vol. 42, no. 5, pp. 1116–1123, 2020.
- [48] R. Lourenzutti and R. A. Krohling, “A generalized TOPSIS method for group decision making with heterogeneous information in a dynamic environment,” *Information Science*, vol. 330, pp. 1–18, 2016.
- [49] Y. Pan and X. Geng, “Hybrid multiple attribute decision making approach based on Mo-RVIKOR,” *Chinese Journal of Management Science*, vol. 27, no. 12, pp. 143–151, 2019.
- [50] F. Wang and H. Li, “Novel method for hybrid multiple attribute decision making based on TODIM method,” *Journal of Systems Engineering and Electronics*, vol. 26, no. 5, pp. 1023–1031, 2015.
- [51] F. Herrera, L. Martínez, and P. J. Sánchez, “Managing non-homogeneous information in group decision making,” *European Journal of Operational Research*, vol. 166, no. 1, pp. 115–132, 2005.
- [52] P. Liu, “A novel method for hybrid multiple attribute decision making,” *Knowledge-Based Systems*, vol. 22, no. 5, pp. 388–391, 2009.
- [53] J. Xu, S. P. Wan, and J. Y. Dong, “Aggregating decision information into Atanassov’s intuitionistic fuzzy numbers for heterogeneous multi-attribute group decision making,” *Applied Soft Computing*, vol. 41, pp. 331–351, 2016.
- [54] S. P. Wan, J. Xu, and J. Y. Dong, “Aggregating decision information into interval-valued intuitionistic fuzzy numbers for heterogeneous multi-attribute group decision making,” *Knowledge-Based Systems*, vol. 113, pp. 155–170, 2016.
- [55] S. P. Wan and J. Y. Dong, *Decision Making Theories and Methods Based on Interval-Valued Intuitionistic Fuzzy Sets*, Springer, 2020.
- [56] Z. Pawlak, “Rough sets,” *International Journal of Computer and Information Sciences*, vol. 11, no. 5, pp. 341–356, 1982.
- [57] M. J. Benítez-Caballero, J. Medina, E. Ramírez-Poussa, and D. Ślęzak, “Rough-set-driven approach for attribute reduction in fuzzy formal concept analysis,” *Fuzzy Sets and Systems*, vol. 391, pp. 117–138, 2020.
- [58] F. Wang, Q. Wu, L.-G. Zhou, and H.-Y. Chen, “An approach to multiple attribute group decision making based on the continuous intuitionistic trapezoidal fuzzy similarity measure,” *Fuzzy Systems and Mathematics*, vol. 32, no. 3, pp. 144–154, 2018.
- [59] T. Wu, L. Bai, E. Liu, and X. Sun, “New entropy formula of intuitionistic fuzzy sets and its application,” *Computer Engineering and Applications*, vol. 49, no. 23, pp. 48–51, 2013.
- [60] X. Quan, “An improved formula of intuitionistic fuzzy entropy,” *Computer Engineering and Software*, vol. 36, no. 10, pp. 40–42, 2015.
- [61] D. L. Xu, G. McCarthy, and J. B. Yang, “Intelligent decision system and its application in business innovation self assessment,” *Decision Support Systems*, vol. 42, no. 2, pp. 664–673, 2006.
- [62] Y. Zhang and G. Chi, “An evaluation and empirical analysis of urban economic and social development based on the set pair analysis,” *Science Research Management*, vol. 40, no. 11, pp. 46–56, 2019.
- [63] G. H. Chen, M. J. Li, and Y. T. Chen, *Research on Combinatorial Evaluation and Its Computer Integrated System*, Tsinghua University Press, 2007.
- [64] F. M. Zhang, *Method of the Combination Evaluation and Its Application*, Science Press, 2018.
- [65] J. Song and C. Chu, “Research on the evaluation system of service enterprise competitiveness,” in *ICSSSM11*, pp. 1–6, Tianjin, 2011.

Research Article

A Compact FPGA-Based Accelerator for Curve-Based Cryptography in Wireless Sensor Networks

Miguel Morales-Sandoval ¹, Luis Armando Rodriguez Flores,² Rene Cumplido,²
Jose Juan Garcia-Hernandez,¹ Claudia Feregrino,² and Ignacio Algreto²

¹Centro de Investigacion y de Estudios Avanzados-Cinvestav Tamaulipas, Mexico

²Instituto Nacional de Astrofisica, Optica y Electronica-INAOE, Mexico

Correspondence should be addressed to Miguel Morales-Sandoval; miguel.morales@cinvestav.mx

Received 17 April 2020; Revised 12 September 2020; Accepted 30 November 2020; Published 6 January 2021

Academic Editor: Iftikhar Ahmad

Copyright © 2021 Miguel Morales-Sandoval et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The main topic of this paper is low-cost public key cryptography in wireless sensor nodes. Security in embedded systems, for example, in sensor nodes based on field programmable gate array (FPGA), demands low cost but still efficient solutions. Sensor nodes are key elements in the Internet of Things paradigm, and their security is a crucial requirement for critical applications in sectors such as military, health, and industry. To address these security requirements under the restrictions imposed by the available computing resources of sensor nodes, this paper presents a low-area FPGA-prototyped hardware accelerator for scalar multiplication, the most costly operation in elliptic curve cryptography (ECC). This cryptoengine is provided as an enabler of robust cryptography for security services in the IoT, such as confidentiality and authentication. The compact property in the proposed hardware design is achieved by implementing a novel digit-by-digit computing approach applied at the finite field and curve level algorithms, in addition to hardware reusing, the use of embedded memory blocks in modern FPGAs, and a simpler control logic. Our hardware design targets elliptic curves defined over binary fields generated by trinomials, uses fewer area resources than other FPGA approaches, and is faster than software counterparts. Our ECC hardware accelerator was validated under a hardware/software codesign of the Diffie-Hellman key exchange protocol (ECDH) deployed in the IoT MicroZed FPGA board. For a scalar multiplication in the *sect233* curve, our design requires 1170 FPGA slices and completes the computation in 128820 clock cycles (at 135.31 MHz), with an efficiency of 0.209 kbps/slice. In the codesign, the ECDH protocol is executed in 4.1 ms, 17 times faster than a MIRACL software implementation running on the embedded processor Cortex A9 in the MicroZed. The FPGA-based accelerator for binary ECC presented in this work is the one with the least amount of hardware resources compared to other FPGA designs in the literature.

1. Introduction

Nowadays, the computing paradigm of Internet of Things (IoT) is enabling a large number of applications in wireless technologies such as smart vehicles, smart buildings, health monitoring, energy management, environmental monitoring, food supply chains, and manufacturing [1].

In critical IoT applications, as in the Industrial Internet of Things (IIoT) or in healthcare (Medical Internet of Things—MIoT), embedded system devices have become an integral part [2] and easy targets of attacks, mainly because they are physically more accessible. Cyberphysical systems

in these domains create new classes of risks resulting from their interaction between cyberspace and the physical world. Wireless sensor networks (WSN) are the cornerstone for realizations of IoT applications, where in some cases, the data generated, stored, or transmitted by the nodes (i.e., embedded systems) require robust security mechanisms to provide them with security services of confidentiality, authentication, integrity, and nonrepudiation. Consider the model for a set of networked IoT devices (for example, a wireless sensor network) in Figure 1. Security risks arise since a malicious node can get unauthorized access to (sensible) data, maliciously alter data, and impersonate legitimate nodes, thus posing

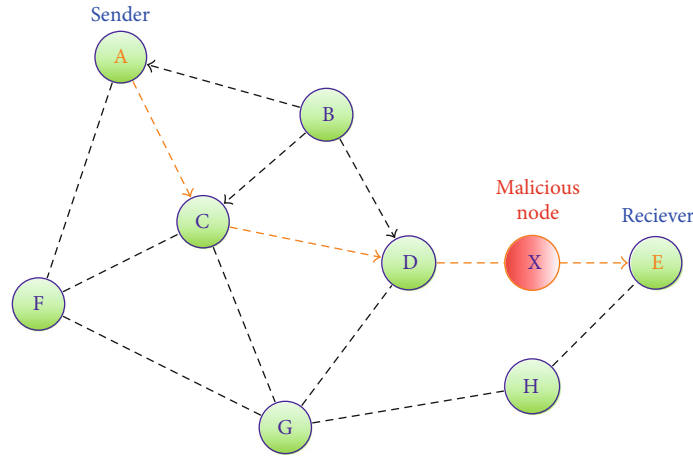


FIGURE 1: Simplified model of networked IoT devices collecting and sharing data.

threats to confidentiality and authentication in the communication path between a sender and a receiver node.

A robust approach to provide such security services in the IoT domain is the public key cryptography (PKC). PKC in its different families is based on mathematical problems, and underlying realizations involve costly arithmetic algorithms over finite fields, rings, or groups. In the literature, a vast amount of research has focused in hardware acceleration of PKC at the different levels of involved arithmetic algorithms. The main approaches for hardware implementations of PKC have focused on speeding up the underlying group and finite field operations at the expense of a high amount of hardware resources. However, the main drawback with hardware for PKC in WSN is the long key lengths which amount to large chip area, circuit delays, and increased power dissipation [3].

The hardware implementation of PKC-based security solutions in resource-constrained devices typically found in IoT scenarios, as in FPGA-based sensor nodes, and using a straightforward approach is not viable. Lightweight cryptography (LWC) [4] has emerged as an active research line focused on designing cryptographic primitives, schemes, and protocols tailored to constrained devices as sensor nodes in WSN or other IoT devices, for example, RFID tags [5]. For the case of PKC, elliptic curve cryptography (ECC) has been considered one of the most efficient realizations well suited for constrained environments in the IoT [6].

Application-specific integrated circuits (ASICs) were the first targets in LWC [4, 7]. However, reconfigurable logic circuits, specifically field programmable gateway arrays (FPGAs), are being more popular to implement compact/low-area hardware accelerators for cryptography algorithms, with attractive advantages for the IoT domain [8]. At the beginning, FPGAs were frequently used as devices for rapid prototyping of cryptographic algorithms, but now they are commonly used as final product platforms [9]. Furthermore, FPGAs are not only used as single parts of embedded systems but rather as system-on-chip (SoC) platforms for implementing complete applications [10]. Modern, commercial FPGA devices contain not only programmable hardware resources but large functional blocks, such as high-speed multipliers, embedded multiport memories, and even

programmable processor cores, thus enabling hardware/software codesigns where the critical parts of algorithm, protocol, or application are accelerated with custom designs implemented in the available programmable hardware, and the rest of the application is executed by the general purpose processors. The main advantage of FPGAs is reconfigurability since, for example, a whole system could be upgraded (or partially reconfigured) [7].

Recent works propose FPGAs as the most attractive candidates to a large range of IoT applications because of their high energy efficiency and low cost, for example, for IoT machine learning [11], IoT neural networks [12], IoT vehicle monitoring systems [13], IoT security (cryptography) [14], and among other applications. Not only research papers propose FPGAs as hardware modules for IoT scenarios but also FPGA vendors are producing devices with specific features for IoT development [15].

Contribution: in this work, we aim at approaching low-area hardware engine to ECC for IoT security, suitable for being included as a building block in FPGA-based sensor nodes for IIoT or MIoT. We aim at providing one of the most compact FPGA hardware accelerator for the scalar multiplication in binary standard curves, the most time consuming operation, and the core of ECC cryptographic schemes such as encryption, digital signatures, and key establishment. To achieve compactness, a novel digit-digit binary finite field multiplier is proposed and used as the basic building block of the proposed ECC accelerator. Under this approach, the operands are processed one digit at a time in an iterative way, but exploiting the parallelism at the algorithmic level and reusing hardware resources as much as possible. The sequence of field operations in the algorithm for scalar multiplication is carefully scheduled to reduce the number of field multiplier cores (two) and memory blocks (eight). While the field multipliers are implemented using standard FPGA logic, memories are taken from the ones available in modern FPGAs. Due to the digit-digit computation approach, an efficient data memory management is designed to reduce the number of memory block. This way, with only the eight memory blocks, the several field multiplications in a single point addition are correctly computed, and at the same

time, those same memories serve to keep the progress of the scalar multiplication computation. The novel hardware design presented in this work was validated under a hardware/software implementation of elliptic curve Diffie-Hellman (ECDH) key exchange protocol, tailored to the MicroZed FPGA prototyping board, recommended for IoT industrial applications. Under this setting, which is very common in an FPGA IoT application, the execution of ECDH outperforms the software counterpart, implemented using the MIRACLE library and runs in the embedded Cortex A9 processor in the MicroZed. Our hardware architecture, compared with state-of-the-art similar approaches in terms of area, only requires up to 16% of FPGA hardware resources, thus being the most compact FPGA-based hardware architecture for computing scalar multiplications in ECC defined over binary fields. Compared to the software reference implementation, our design is 17 times faster.

The rest of this brief is organized as follows: *Materials and Methods* discusses the preliminaries of scalar multiplication in binary elliptic curves and the Montgomery López-Dahab algorithm for scalar multiplication. This section also describes related works and the proposed hardware design. *Results and Discussion* presents the experimental results and comparisons with state-of-the-art works, followed by concluding remarks in the *Conclusion*.

2. Materials and Methods

First, we provide the mathematical concepts and foundations that are the basis to construct the FPGA-based ECC cryptoengine. First, we present the basis of elliptic curves and groups from which the scalar multiplication is defined. Scalar multiplication is critical because the proposed hardware cryptoengine is precisely to speed up this costly operation and the core of higher operations for security applications such as encryption and digital signatures. Finally, the section concludes discussing the method to compute scalar multiplications on binary elliptic curves. This algorithm is realized by the proposed FPGA-based ECC cryptoengine.

2.1. Elliptic Curves and Its Use in Cryptography. Since invented independently by Miller [16] and Koblitz [17], elliptic curve cryptography (ECC) has received a lot of attention in the academy and industry. Elliptic curves and their properties have enabled also other types of cryptography relevant for the IoT (in wireless sensor networks), for example, identity-based encryption (IBE) [18] and attribute-based encryption [19]. With the advent of the IoT, mainly plagued by intelligent object with restricted computing and resources capabilities, ECC is becoming one of the promising approaches to provide security services in that computing paradigm [6].

An elliptic curve \mathbb{E} over a finite field \mathbb{F}_q is defined by Eq. (1).

$$\mathbb{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$. The (x, y) pairs satisfying \mathbb{E} , together with a special point named point at infinity O , form

a group \mathbb{G} with point addition as the group operation. \mathbb{G} is a cyclic group with prime order n where the discrete logarithm problem is defined and on which ECC is founded.

It is well known that binary extension fields ($q = 2^m$) are very attractive for defining ECC. An element in \mathbb{F}_{2^m} is the bit vector $(a_{m-1}, a_{m-2}, \dots, a_0)$ that in polynomial basis represents the $(m-1)$ -degree polynomial $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_0$, with a_i in $\{0,1\}$. Arithmetic in \mathbb{F}_{2^m} in polynomial basis is polynomial arithmetic with reduction modulo, which is an irreducible polynomial of degree m , $F(x)$. The arithmetic in \mathbb{F}_{2^m} is carry free and more suitable for hardware implementations.

2.2. Scalar Multiplication in Elliptic Curves. Scalar multiplication in $\mathbb{E}(\mathbb{F}_q)$ denoted as $Q = kP$ with $Q, P \in \mathbb{G}$ and $k \in [1, n-1]$ is the main and most time-consuming operation in any ECC scheme (encryption, digital signature, keys exchange, etc). Q is computed by k -times point addition operations of P with itself [20]: $Q = kP = \underbrace{P + P + \dots + P}_{k\text{-times}}$.

The complexity of kP is in terms of the operations in \mathbb{F}_q . Given a large integer k and a point P in \mathbb{G} , it is easy to compute $Q = kP$. On the contrary, the elliptic curve discrete logarithm problem (ECDLP) is the problem that given the point P and Q in \mathbb{G} , to find the scalar k . For an enough large n , ECDLP becomes hard to solve. Most of the state-of-the-art works related to ECC have been focused on the efficient implementation of scalar multiplication [6], which is a condition for efficient ECC implementation.

The Lopez-Dahab Montgomery PM algorithm [21], shown in Algorithm 1, has been commonly used for the kP computation because it is side-channel attack-resistant, suitable for parallelization and low resource friendly. In this work, we use the Lopez-Dahab algorithm for implementing for the first time the most compact FPGA-based hardware architecture for computing kP in binary elliptic curves, $\mathbb{E}(\mathbb{F}_{2^m})$.

The main operations in Algorithm 1 are addition, multiplication, and squaring in \mathbb{F}_{2^m} . Consider the fields recommended by NIST for practical ECC, with $m = 233$ and $m = 409$. For $m = 409$, 2.2 will have a cost of 1227 field additions, 2454 field multiplications, and 2454 field squarings over \mathbb{F}_{2^m} , being field multiplication the most time-consuming operation.

The Lopez Dahab's method for scalar multiplication in ECC is considered as the most suitable method when targeting low computing powered devices [22]. The elliptic curve point is represented in projective coordinates. At the beginning, the elliptic curve point P in affine coordinates (x, y) is converted to its projective representation (X, Y, Z) . Algorithm 1 uses the x -coordinate only for point representation so storage resources can be saved (line 5). With this setting, costly field inversions are avoided in each group (curve level) operation. Only one field inversion is required for coordinate conversion from projective to affine at the end of the main loop (line 13). Algorithm 1 is time-constant and resistant to some side-channel attacks such as simple power analysis (SPA).

```

 $E(\mathbb{F}_{2^m})$ 
Require:  $k \geq 0$ 
Require:  $P = (x, y) \in E(\mathbb{F}_{2^m})$ 
1: function MONTGOMERYk, P
2:   if  $k = 0$  or  $x = 0$  then
3:     return  $(0, 0)$ .
4:   end if
5:    $P_1(X_1, Z_1) \leftarrow (x, 1); P_2(X_2, Z_2) \leftarrow (x^4 + b, x^2)$ 
6:   for  $i$  from  $l - 2$  downto 0 do
7:     if  $k_i = 1$  then
8:        $P_1 \leftarrow \text{Madd}P_1, P_2; P_2 \leftarrow \text{Mdouble}(P_2)$ 
9:     else
10:       $P_2 \leftarrow \text{Madd}P_2, P_1; P_1 \leftarrow \text{Mdouble}(P_1)$ 
11:    end if
12:  end for
13:  return  $Q = \text{Mxy}(P_1, P_2, P)$ 
14: end function
1: procedure MADD $P_1, P_2$ 
2:   $Z_3 \leftarrow (X_1Z_2 + X_2Z_1)^2; X_3 \leftarrow xZ_3 + X_1X_2Z_1Z_2$ 
3:  return  $P_3(X_3, Z_3)$ 
4: end procedure
1: procedure MDOUBLE $P_1$ 
2:   $Z_2 \leftarrow X_1^2Z_1^2, X_2 \leftarrow X_1^4 + bZ_1^4$ 
3:  return  $P_2(X_2, Z_2)$ 
4: end procedure
1: procedure GXP $P_1, P_2$ 
2:   $x_q \leftarrow X_1Z_1^{-1}$ 
3:   $Y_{int} \leftarrow (X_1 + xZ_1)(X_2 + xZ_2) + (x^2 + y)Z_1Z_2$ 
4:   $y_q \leftarrow (x + x_q)Y_{int}(xZ_1Z_2)^{-1} + y$ 
5:  return  $Q(x_q, y_q)$ 
6: end procedure

```

ALGORITHM 1: Montgomery scalar multiplication [21].

2.3. Related Work. Being kP the core operation in ECC cryptographic schemes, that operation has been the main target for hardware accelerations; however, few works have approached low-area designs compared to those trying to achieve the maximum performance. However, for the devices used in the IoT, generally sensor nodes, lightweight realizations of cryptography are better preferred to efficiently use the available computing and power resources in the sensor nodes [23].

The computation of kP implies to execute a scalar multiplication algorithm, being Algorithm 1 one of the most recommended. At each iteration, curve (group) arithmetic is executed, either point addition or point doubling, each implying several finite field operations. So, operations in groups and finite fields are critical for public key cryptography as in elliptic curve cryptography (ECC). An efficient implementation of kP requires an efficient implementation of finite field operations, being multiplication and inversion the most time consuming field operators. Field inversion can be efficiently realized through several field multiplications; consequently, hardware field multiplier has been studied as the main core to compute kP .

In the case of \mathbb{F}_{2^m} , there are three main families of algorithms to compute a field multiplication $A(x) \times B(x) \bmod F(x)$: full-parallel, bit-serial, and digit-serial [24]. The full-

parallel approach is the most costly in terms of area usage but is the fastest while the bit-serial approach is generally the most compact but its slower. The digit-serial approach allows a trade-off between computation time and area usage.

Related works are discussed in this section, based on the type of multiplier being used (bit-serial, digit-serial), computing approach (LSE, MSE), the implementation platform (FPGA type), the finite field size, and implementation results in terms of time and area (FPGA slices). Note that our contribution is on the multiplier being used and in the computing approach (digit-digit). This approach has not been explored, and we present for the first time an FPGA accelerator for ECC based on such approach.

Digit-serial and bit-serial approaches to field multiplication are iterative algorithms that process one of the operands in the multiplication from right-to-left (MSE) or from left-to-right (LSE). At each iteration, the partial results need modular reduction. Bertoni et al. [25] presented an easy way to perform modulo reduction when partial results have coefficients with powers greater than $m - 1$ (e.g., a^m). Beuchat et al. [24] surveyed some of the most representative \mathbb{F}_{2^m} implementations using MSE and LSE algorithms (including implementations presented in [25]).

Digit-serial implementations (with digit size D) require $\lceil m/D \rceil$ iterations using $(m - 1)$ -degree partial results [26]. However, in [27], it is proposed to use $(m + D - 1)$ -degree partial results to improve computation performance at the cost of one extra iteration, requiring $m + 1$ iterations to compute multiplication over \mathbb{F}_{2^m} . The digit-serial algorithm proposed in [25] requires $m + 1$ iterations and keeps $(m + D - 1)$ -degree partial results to improve computation performance. Beuchat [24] concluded that the MSE first approach requires less hardware and offers higher throughput than LSE. In [28], the reduction steps are performed separately. It is stated that for a finite field generated by irreducible polynomials $F(x)$ (NIST [29]), reduction can be performed by a set of *xor* operations [30, 31]. [28] is considered only the multiplication step, implemented in a digit-serial approach. A digit $D = 16$ is proposed since in most cases, 16-bit words give better results.

In [32], it is used a LSE digit-serial multiplier; however, a digit size of one bit (bit-serial) resulted the most compact version. [33] is proposed a systolic hardware architecture to compute multiplication/inversion in the same hardware. Furthermore, an arithmetic unit is constructed that can perform all \mathbb{F}_{2^m} arithmetic operations required in elliptic curve cryptography. [34] is presented for the first time a digit-digit \mathbb{F}_{2^m} multiplier under a MSE basis. Operands, modulus, and partial results are partitioned in digits and processed one digit at a time. The main advantage compared to digit-serial or bit-serial implementations is that operands and partial results can be stored in BRAMs instead of shift registers which saves standard logic (slices). However, the multiplier presented is designed and evaluated as a standalone module which is hard to directly use in a kP engine.

Table 1 summarizes the most relevant works for \mathbb{F}_{2^m} multiplication in FPGA, the main algorithms used, and the area/time results. Table 2 shows some of the most representative works of hardware designs for kP computation in the

TABLE 1: Hardware approaches for \mathbb{F}_{2^m} multipliers.

Ref.	Field	Target	Algorithm	Approach	Slices	Time (ns)
[24]	$F(2233)$	Spartan 3	MSE	Digit-serial	3458	58.0
[24]	$F(2233)$	Spartan 3	LSE	Digit-serial	3504	62.0
[24]	$F(2409)$	Spartan 3	MSE	Digit-serial	5406	153.0
[28]	$F(2233)$	Virtex 6	Schoolbook method	Digit-serial	1643 (LUTs)	802.4
[32] ($d=1$)	$F(2233)$	Virtex 5	LSE	Digit-serial	714 (LUTs)	415.0
[32] ($d=16$)	$F(2233)$	Virtex 5	LSE	Digit-serial	2351 (LUTs)	35.0
[34]	$F(2233)$	Spartan 3	MSE	Digit-digit	406	219.0
[33]	$F(2163)$	Virtex II	M-I algorithm	Systolic array	1399	

TABLE 2: Hardware approaches for kP in FPGAs.

Ref.	Field	Target	Mult. algorithm	Approach	Slices	Time
[4]	$F(2193)$	ASIC	MSE	Digit-serial	17723 GE	41.70 ms
[32]	$F(2233)$	Virtex 5	MSE	Digit-serial	6487	19.89 μ s
[38]	$F(2233)$	Virtex 7	MSE	Digit-serial	2647	16.01 μ s
[39]	$F(2163)$	Spartan 3	LSE	Bit-serial	3383	2.23 ms
[40]	$F(2193)$	Spartan 3	Comba wxw	Digit-serial	473	125.00 ms
[37]	$F(2233)$	Kintex 7	MSE	Bit-serial	3016	2.66 ms
[41]	$F(2163)$	Virtex 5	Karatsuba	Bit-parallel	3789	10.00 μ s

hardware. Most of the reported works use the bit-serial or digit-serial approach to implement hardware \mathbb{F}_{2^m} operators. However, hardware resources required in these approaches depend directly on the operands size (field size m), because even when one of the operands is iteratively processed, the other one is processed in parallel.

The bit-serial approach requires small amount of hardware resources compared to the digit-serial or full-parallel approach, but for large operands, even using the bit-serial approach requires a considerable amount of hardware resources (slices). However, some recent works already proposed using a digit-digit approach, for example, [34, 35]. The main drawback with the multiplier presented in [34] is the use of shift registers to store partial results and the infeasibility of using such design for practical kP engine and for [35] is to fit the digit sizes to FPGAs embedded DSP multipliers.

In order to reduce area requirements and achieve a compact design well suited for IoT applications, the approach in this work to construct a hardware kP accelerator follows the digit-digit computation approach and makes use of multipliers and memory blocks embedded in most of the FPGAs to save FPGA standard logic. By implementing a strategy for reusing memory blocks, critical for the iteratively processing of the digit-digit approach, considerable area resources are saved but retaining the advantage of processing iteratively both operand in the multiplication and not only one as in the digit-serial or bit-serial approaches. Additionally, since memory blocks are bigger than operands, it is proposed to used part of the available memory blocks to store control

signals thus (microprogramming) avoiding logic to implement a state machine for control.

2.4. Novel Digit-by-Digit Elliptic Curve Point Multiplication Hardware Architecture. The proposed ECC engine, suitable for FPGA-based sensor nodes in the IoT, is constructed following a layered-based approach. The low level is the \mathbb{F}_{2^m} arithmetic, where field multiplication is the main operation to be optimized in terms of area resources. Next, using the \mathbb{F}_{2^m} multiplier as a building block in the high layer is the curve arithmetic, consisting in the optimized realization of Algorithm 1 in terms of area resources, where the \mathbb{F}_{2^m} multiplier is used to compute each of the point additions (lines 8 and 10). At this level, the \mathbb{F}_{2^m} multiplier is used to realize field inversion and field squaring required in the addition and double point operations. In both layers, the proposed design methodology takes advantage of block RAMs (BRAMs) embedded in modern FPGAs to store the operands, partial, and final results, reusing the BRAMs as much as possible, using a carefully field operation scheduling, and memory management strategy.

2.4.1. Field Arithmetic. Arithmetic in \mathbb{F}_{2^m} is done using polynomial basis. Under this representation, each element in the field is an $(m - 1)$ -degree polynomial $A(x)$ over the field \mathbb{F}_2 . The two \mathbb{F}_{2^m} binary operators are addition and multiplication with reduction modulo which is an irreducible polynomial $F(x)$ of degree m . Field addition is the bit-wise XOR operation of coefficients (carry free, no reduction needed), a cheap

operation when implemented in the hardware. Additive inverse in \mathbb{F}_{2^m} under polynomial basis is also easy to implement, as for any $A(x)$ in \mathbb{F}_{2^m} , $A(x) + A(x) = 0$, with 0 as the neutral addition element (all zero polynomial).

Multiplication and multiplicative inverses (or simply inversion) in \mathbb{F}_{2^m} are more complex operations. Since Algorithm 1 only requires one \mathbb{F}_{2^m} inversion at the end of the computation, field inversion is implemented using the Itoh-Tsuji algorithm, by a series of \mathbb{F}_{2^m} multiplications. So, the field multiplier becomes the most critical operation to be carefully implemented in ECC hardware approaches and one of the critical component in our kP engine.

2.4.2. \mathbb{F}_{2^m} Multiplication. In the literature, there are basically three computing approaches for computing field multiplication in the hardware: bit-serial (the most compact design), digital-serial (for area-performance trade-offs), and full-parallel (the fastest but also the costlier solution in terms of area). The most significant element (MSE) and least significant element (LSE) (bit-serial or digit-serial) are the commonly used algorithms to compute multiplications over \mathbb{F}_{2^m} .

In this work, we propose a novel digit-digit \mathbb{F}_{2^m} multiplier algorithm well suited to be integrated into a kP engine. The digit-digit computing approach aims at performing better than a bit-serial multiplier, keeps the property of allowing exploring area-performance trade-offs when realized in hardware, and it is not as expensive as a full parallel realization. This is consistent with our design methodology to achieve a compact architecture (simpler datapath) for the kP engine. Details of the digit-digit \mathbb{F}_{2^m} multiplier are presented in Section 2.4.3.

\mathbb{F}_{2^m} multiplication using the digit-digit computing approach was previously suggested in [34]. However, the multiplier design in that work is not suitable for a direct application in a kP engine. The authors in that work only proved the advantages of the digit-digit approach versus the well-known bit-serial and digit-serial multipliers, as a standalone module. However, when that multiplier is considered for realizing the kP operation, several issues must be solved.

Being the multiplier part of a series of operations implied by each point addition operation in the main loop in the kP computation, the main challenge for the digit-digit multiplier is the fact that partial results at each iteration in the digit-digit multiplier and the final result (possibly operated with other values) are the input operand for the same multiplier in next iterations. So, during the digit-digit computation, the multiplier must keep its operands in memory blocks M_1 and M_2 and progressively stores the partial results in another one M_3 . At the end, the results in M_3 should be moved to M_1 or M_2 for further processing (a kP operation requires several \mathbb{F}_{2^m} multiplications), introducing a delay in the kP computation, unless that data movement is done during the computation. So, M_1 or M_2 must act as an input and output memory at the same time. Since a complete kP operation requires several hundreds of multiplications, using the multiplier as proposed in [34] without addressing the previous data memory management issue is totally unpractical.

As it is explained in the next section, the main issue to integrate a digit-digit \mathbb{F}_{2^m} multiplier in the kP engine is to

implement an efficient data memory management, ensuring consistency in the correct execution of both the digit-digit field multiplier and the scalar multiplication algorithm. In this work, we present the design of a novel digit-digit \mathbb{F}_{2^m} multiplier that achieves compact designs by optimizing the resources for finite fields defined by trinomials.

2.4.3. Digit-Digit \mathbb{F}_{2^m} Multiplier. Parting from the definition of elements in \mathbb{F}_{2^m} , as polynomials of the form $b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \dots + b_0$ with binary coefficients, in this section, we present how the mathematical expression that computes an \mathbb{F}_{2^m} multiplication in a digit-by-digit fashion is derived (from Eq. (2) to Eq. (9)). This expression leads to the specification of the \mathbb{F}_{2^m} multiplier that is the building block of our FPGA-based engine for scalar multiplication in ECC.

An element $B \in \mathbb{F}_{2^m}$ of the form $b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \dots + b_0$ can be represented as the sum of $w = \lceil m/d \rceil$ polynomials (digits) each of d coefficients in \mathbb{F}_2 (Eq. (2)).

$$B(x) = \sum_{i=0}^{m-1} b_i x^i = \sum_{i=0}^{w-1} B_i x^{id}, B_i = \sum_{j=0}^{d-1} b_{id+j} x^j. \quad (2)$$

So, Eq. (3) expresses the multiplication $C(x) = A(x) \times B(x) \bmod F(x)$ in a digit-serial approach.

$$\begin{aligned} C &= A \times B \bmod F(x) \\ &= \left(A \times \sum_{i=0}^{w-1} B_i x^{di} \right) \bmod F(x) \\ &= AB_0 \bmod F(x) + AB_1 x^d \bmod F(x) \\ &\quad + AB_2 x^{2d} \bmod F(x) + \dots + AB_{w-1} x^{(w-1)d} \bmod F(x). \end{aligned} \quad (3)$$

Let $P^{<i>}(x) = AB_i$, $0 \leq i \leq w-1$, and the $(d+m-2)$ -degree polynomial resulting from the partial product at iteration i in Eq. (3). By parsing elements of B from left-to-right (MSE), C computation at iteration i is determined by recurrence in Eq. (4):

$$C^{<0>} = 0, \quad (4)$$

$$C^{<i+1>} = x^d (C^{<i>} \bmod F(x)) + P^{<w-1-i>}(x), \quad (5)$$

where polynomial $x^d (C^{<i>} \bmod F(x))$ has the most degree $(d+k-1)$, while $P^{<i>}$ is of degree $(d+k-2)$. After w iterations, the polynomial $C^{<w-1>}$ of degree $(d+k-1)$ needs reduction. By introducing an extra iteration with $B_{-1} = 0$ and $P^{<-1>} = 0$, $C^{<w>} = x^d (C^{<w-1>} \bmod F(x))$ is the result. The x^d term in this last expression can be easily reduced modulo $F(x)$ by only discarding the digit $C_0^{<w>}$.

Being $F(x)$ an m -degree polynomial, $F(x) = x^m + \sum_{i=0}^{m-1} f_i \alpha^i$. So, $x^m \bmod F(x) = \sum_{i=0}^{m-1} f_i \alpha^i = g(x)$, a polynomial of degree g with $g < m$. Thus, elements x^{m+t} with $t \leq m-1-g$ can be reduced using equivalence $x^{m+t} \bmod F(x) = g(x)x^t$.

Degree of $C^{<i+1>}$ from Eq. (5) (after $C^{<i>}$ reduction) is at most $(d+m-1)$. This polynomial becomes the $C^{<i>}$ polynomial to be reduced in the next iteration ($C^{<i>} \bmod F(x)$). So,

at each iteration $i + 1$, it is required to reduce the d -terms x^j of $C^{<i>}$, $m - 1 < j \leq d + m - 1$. By using the previous assumption for polynomial reduction being $F(x)$ a trinomial, the reduction in Eq. (5) can be defined as in Eq. (6).

$$\begin{aligned} C^{<i>} \bmod F(x) &= \sum_{i=0}^{m-1} c_i x^i + \left(\sum_{i=m}^{m-1+d} c_i x^i \right) \bmod F(x) \\ &= \sum_{i=0}^{m-1} c_i x^i + \left(\sum_{i=0}^{d-1} c_{m+i} x^i g(x) \right) \bmod F(x) \\ &= C_m^{<i>}(x) + C_d^{<i>}(x) \times g(x). \end{aligned} \quad (6)$$

This way, $C^{<i>}$ is partitioned in two polynomials $C_m^{<i>}(x)$ and $C_d^{<i>}(x)$ of degree $m - 1$ and d , respectively. The partial multiplication $C_d^{<i>} \times g(x)$ will not require modular reduction if $d + g < m$. So, Eq. (5) can be rewritten as in Eq. (7).

$$C^{<i+1>} = \alpha^d (C_m^{<i>} + C_d^{<i>} \times g(x)) + P^{<w-1-i>}. \quad (7)$$

Under the digit-digit computation approach, the polynomial $C_m^{<i>}$, $g(x)$, and A is represented in $w = \lceil md \rceil$ digits. Since the B_i degree is $d - 1$, the $P^{<i>}$ computation can be achieved iteratively, taken digit B_i and iterating through A digits. Taking B_i as a constant, $P^{<i>}(x) = A(x) \times B_i(x) = \sum_{j=0}^{w-1} (A_j \times B_i) x^{jd} = \sum_{j=0}^{w-1} P_j^{<i>} x^{jd}$. With this new notation, the first term in Eq. (4) can be rewritten as in Eq. (7).

$$\begin{aligned} x^d (C_m^{<i>}(x) + C_d^{<i>}(x) \times g(x)) &= \sum_{j=0}^{w-1} C_j^{<i>} x^{jd+d} + C_d^{<i>}(x) \times \sum_{j=0}^{w-1} G_j x^{jd+d} \\ &= \sum_{j=0}^{w-1} (C_j^{<i>} + C_d^{<i>}(x) \times G_j) x^{jd+d} \\ &= \sum_{j=0}^{w-1} R_j^{<i>} x^{jd+d}. \end{aligned} \quad (8)$$

Once $P^{<i>}$ and $R^{<i>}$ are expressed to be processed in an iterative way one digit at a time, Eq. (7) can be rewritten in a notation that leads to an iterative, digit-by-digit computation of each partial product of \mathbb{F}_{2^m} multiplication, given by Eq. (9).

$$C^{<i+1>} = \sum_{j=0}^{w-1} (R_j^{<i>} \alpha^{jd+d} + P_j^{<i>} \alpha^{jd}). \quad (9)$$

At each iteration, values $P_j^{<i>}$ and $R_j^{<i>}$ can be computed in a parallel way. For the sake of clarity about the computations in Eq. (9), the sum of digits $P_j^{<i>}$ and $R_j^{<i>} x^d$ can be expressed as a single variable $S_j^{<i>}$. This new variable $S_j^{<i>}$ is $(d + d + d)$ bits in size as shown in Figure 2.

With all these considerations, the proposed algorithm for computing multiplication over \mathbb{F}_{2^m} is presented in Algorithm 2.

2.4.4. Digit-Digit \mathbb{F}_{2^m} Multiplier Hardware Architecture. To achieve compactness, in this work, we propose the realization in hardware of Algorithm 2 in its simplest form. The hardware architecture only requires one partial $d \times d$ multiplier and is optimized for binary fields defined by a trinomial. The NIST and other compliant standards have recommended trinomials for binary fields, for example, $F(x) = x^{409} + x^{87} + 1$ and $F(x) = x^{233} + x^{74} + 1$.

If the 233-degree trinomial is used, $g(x) = x^{74} + 1$ is used for the reduction step. So, if $d = 74$ (digit size) is used, when a digit j of $g(x)$ (G_j) is read, only the two first digits will have a value of 1, when $j > 1$ digit G_j will be always 0. In this case, the partial multiplier that computes $C_d^{<i>}(x) \times G_j$ always computes a multiplication of the form $(C_d^{<i>}(x) \times 1)$ or $(C_d^{<i>}(x) \times 0)$ which can be implemented only with an “and” gate. In conclusion, when a trinomial of the form $x^m + x^k + 1$ is used, it is possible to define the digit size $d = k$. In this case, the partial multiplier that computes $C_d^{<i>}(x) \times G_j$ can be implemented using only a multiplexer as it is shown in Figure 3.

2.4.5. Curve Arithmetic. The hardware for elliptic curve scalar multiplication is guided by the execution of Algorithm 1, which is based on the iteratively call to point addition functions *Madd* and *Mdouble*.

Figure 4 shows the required operations at each iteration of Algorithm 1 and the underlying \mathbb{F}_{2^m} operations (denoted by circles). After each \mathbb{F}_{2^m} operation, the figure also shows the memory where the intermediate values are stored. For example, the memory *X11* stores the first field operation $X_1 \times Z_2$ in the point addition operation. While five \mathbb{F}_{2^m} multiplications are needed to compute a single *Madd* operation, six \mathbb{F}_{2^m} multiplications are required for *Mdouble*.

The schedule of field operations shown in Figure 4 considers only the use of four memories to compute the complete *Madd* function, by reusing the memory blocks properly. For the case of *Mdouble*, also four memories are enough. The memories are alternatively used as shown in the figure to act as the repository for the input parameters to a field multiplier/adder or as the repository for the multiplication/addition result. We stress again the fact that a proper data memory management must be implemented to avoid the delays induced by moving data from the result memory to the input parameter memory in the chained \mathbb{F}_{2^m} operations.

Since in Algorithm 1, only the X and Z coordinates of elliptic curve points in projective representation are used, and each point $P(X, Z)$ is stored in two BRAMs, one for the X and the other for the Z coordinate. In Figure 4, the memories for the points P_1 and P_2 are represented by the variables X_1, X_2, Z_1, Z_2 .

For *Madd*, let us consider the first multiplication $X_1 \times Z_2$ stored in *X11* and the second multiplication $X_2 \times Z_1$ stored in *Z11*. Both multiplications can be done in parallel, with memories X_1, X_2, Z_1, Z_2 acting as reading memories and X_11 and $Z11$ acting as the writing memories. For the third multiplication $X11 \times Z11$, memories *X11* and *Z11* must switch to act as reading memories, and the result can be stored in *Z1*, the memory that initially stored one of the input

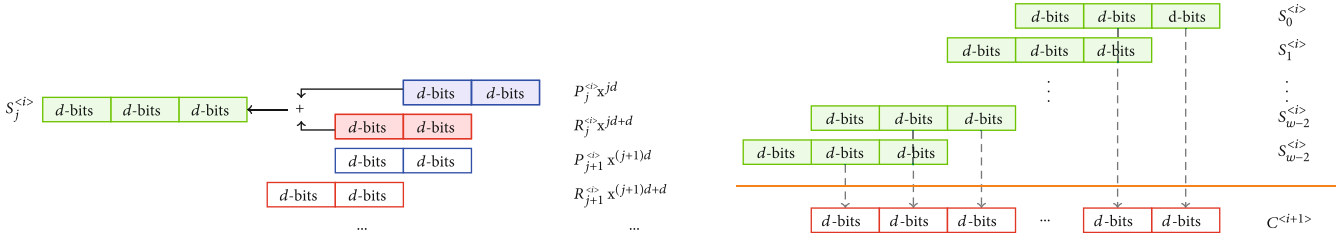


FIGURE 2: Digit-digit computation of \mathbb{F}_2m multiplication.

```

Require:  $A, B, F \in \mathbb{F}_2m$     $\triangleright A = \sum_{i=0}^{w-1} \alpha_i \alpha^{iD}$     $\triangleright B = \sum_{i=0}^{w-1} b_i \alpha^{iD}$ 
1:  $cD \leftarrow 0$ 
2: for  $i \leftarrow 0$  to  $w + 1$  do
3:    $carry \leftarrow 0$ 
4:    $s \leftarrow 0$ 
5:   for  $0 \leftarrow 0$  to  $wD$  do
6:      $P_i \leftarrow b_{digits-i} \times \alpha_j + 1$ 
7:      $R_j \leftarrow c_j + cD \times f_j + 1$ 
8:      $s \leftarrow P_i + (R_j \ll d) + carry$ 
9:      $c_j \leftarrow s[d - 1 \text{ downto } 0]$ 
10:     $cD \leftarrow s \gg d$ 
11:   end for
12:   $cD \leftarrow s \gg bitsLastDigit$ 
13: end for
14:  $c_w \leftarrow carry$ 
15: return    $\triangleright c = A \times B \text{ mod } F$     $\triangleright c = \sum_{i=0}^{w-1} c_i \alpha^{iD}$ 

```

ALGORITHM 2: Digit-digit \mathbb{F}_2m multiplier algorithm.

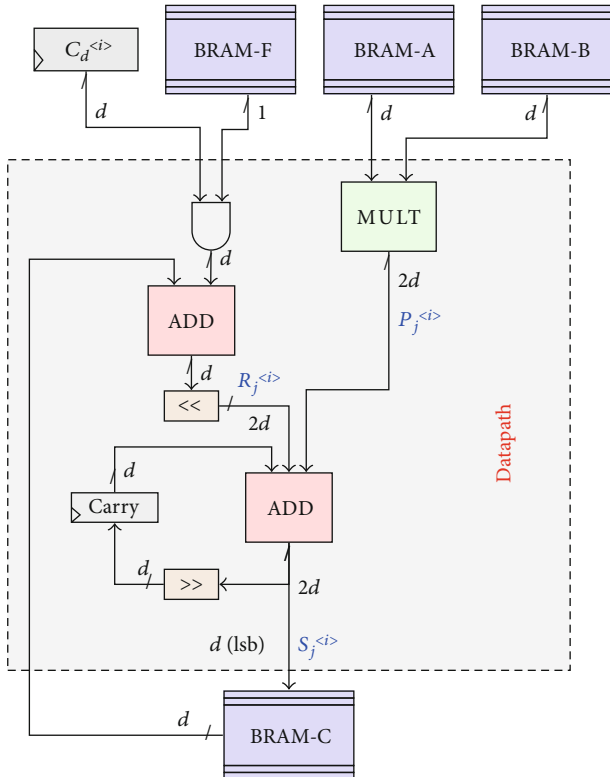


FIGURE 3: Hardware architecture \mathbb{F}_2m .

parameters and now acts as a writing memory. As the \mathbb{F}_2m multiplier delivers a result at each stage in point addition, at the same time, it processes the input digits. So, a careful management of the memory is required to avoid latency for data movement for result and input parameter memories. This requirement arises because the result of the field multiplier in an earlier stage becomes the input parameter of later stages.

In the rest of the point addition computation, memories alternate their functionality following the switching strategy of read/write memories. At the end, the final result X_3, Z_3 must be in a memory, that is used in the next iteration at line 6 in Algorithm 1, so that values will reside in one of the four available memories, and input parameters in next iteration in the main loop of Algorithm 1 are adjusted. Memories associated to points $P1(X_1, Z_1)$ and $P2(X_2, Z_2)$ are overwritten with new partial results coming from the $Madd$ and $Mdouble$ functions.

At line 8 (or also in line 10) in the main loop of Algorithm 1, the memories storing $P_1(X_1, Z_1)$ and $P_2(X_2, Z_2)$ are read memories, and the result is stored finally in memories $P11(X11, Z11)$ and $P22(X22, Z22)$ (see Figure 4). In the next iteration, $P11(X11, Z11)$ and $P22(X22, Z22)$ become P_1 and P_2 input parameters, and the corresponding memories $P_1(X_1, Z_1)$ and $P_2(X_2, Z_2)$ become the storage for the result of the final point addition. So, at the curve level

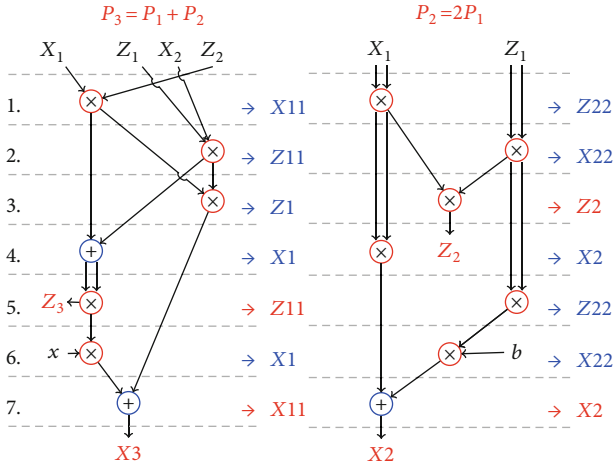


FIGURE 4: Proposed schedule for point addition/double in $E(\mathbb{F}_2m)$.

algorithm, the memories are also interchanged in their functionality and properly mapped to the memories for the final results in Figure 4. An extra BRAM is required to store the scalar k .

The building blocks to compute kP as described in Figure 4 are those for field arithmetic operations: addition, multiplication, square, and inversion over \mathbb{F}_{2^m} . The square operation is considered easier than multiplication. However, since in this work operands are stored in BRAMs, and reading/writing of operands are performed one digit at a time, it is difficult to take advantage of the optimized algorithm such as the fast reduction algorithm proposed by NIST commonly used in squaring. So, to save hardware resources, this work uses one \mathbb{F}_{2^m} multiplication core to compute square operations. The reusing of the multiplier saves area but increases latency. Also, \mathbb{F}_{2^m} inversion is computed with the Itoh-Tsujii algorithm by means of multiplications, squares, and additions in \mathbb{F}_{2^m} .

At each iteration of Algorithm 1, $Madd$ and $Mdouble$ operations can be computed in parallel since there is no data dependency. In this work, we propose to use a \mathbb{F}_{2^m} multiplier in $Madd$ and other in $Mdouble$ to take advantage of parallelism. In the dataflow for each point addition, the \mathbb{F}_{2^m} multiplier is reused. In addition to the multipliers, one \mathbb{F}_{2^m} adder is also required. The same adder can be used in both the $Madd$ and $Mdouble$ operations since it is required at different times in each operation.

Although more than one \mathbb{F}_{2^m} multiplier could be added to speed up the kP computation, that approach resulted in extra cost of hardware resources not only because of the area required by the \mathbb{F}_{2^m} multiplier but also for the increased complexity in the control module and additional multiplexers to manage input/output operands to the \mathbb{F}_{2^m} cores.

The entire kP dataflow is managed by a control unit that stimulates the memory blocks for word-based reading and writing and also commands the \mathbb{F}_{2^m} cores (multipliers and adder). The control module waits until each partial multiplication/addition has finished and starts the following required operations with the correct BRAM as input sources.

3. Results and Discussion

The proposed compact hardware ECC design was implemented over the binary fields $\mathbb{F}_{2^{233}}$ and $\mathbb{F}_{2^{409}}$, both defined by an irreducible trinomial. The elliptic curves used were sect233 and sect409, both recommended by NIST and other recognized organizations such as SECG. The target platform was the IoT recommended FPGA board MicroZed, with Xilinx Vivado HLx 2016.4 as the developer tool.

The hardware architecture for scalar multiplication in $E(\mathbb{F}_{2^m})$ was evaluated in a hardware-software codesign of the Diffie-Hellman key exchange elliptic curve (ECDH) version. Let it consider that two FPGA-based sensor nodes [36] A and B agree on an elliptic curve group \mathbb{G} with generator P and order n . Then, each party selects a secret integer, for example, r_A and r_B . Using a kP engine, each party computes public values:

$$\underbrace{Q_A}_{\text{Sensor A}} = r_A P \text{ and } \underbrace{Q_B}_{\text{Sensor B}} = r_B P. \quad (10)$$

Sensor A uses the B 's public value to compute $s_1 = r_A Q_B$, and the sensor B uses the A 's public value to compute $s_2 = r_B Q_A$. Since s_1 is the same as s_2 ($s = s_1 = s_2$), s acts as a shared secret key between the sensors A and B , so a secure channel can be established to transport data between the two devices in an encrypted form (for example, using a lightweight block cipher). Indeed, signatures can be generated to authenticate data by using the secret to authenticate a message, using, for example, LightMac. The main complexity in ECDH (as in other ECC-based cryptographic schemes) is the computation of kP .

3.1. Hardware/Software Codesign. Figure 5 shows the proposed hardware-software codesign for the scalar multiplier over $E(\mathbb{F}_{2^m})$, suitable to be realized in an FPGA sensor node. The codesign was realized in the MicroZed board, and the implementation results are shown in Table 3. This is a representative final application under an IoT scenario (IIoT, MIoT) where sensor nodes are deployed using SoC technology: the kP scalar multiplication is executed in FPGA technology coupled to a master general purpose processor that runs the rest of the application logic. The hardware-software codesign required 1809 slices of the FPGA embedded in the MicroZed board running at 62.5 MHz.

Table 3 also compares the time to achieve a scalar multiplication under the hardware/software codesign versus a pure software implementation. This is done to highlight the gain in performance from a hardware approach for the most time-consuming operation in ECC, as in ECDH. For this, we used the MIRACL library for the software implementation of scalar multiplication in the Cortex A9 of the Zynq, also available in the MicroZed board. In this case, we used the same implementation parameters: curve, finite field, size of the finite field, irreducible polynomial, projective coordinates, and the same Algorithm 1 for scalar multiplication.

The hardware-accelerated execution of kP requires 4.13 ms to compute an elliptic curve Diffie Hellman key

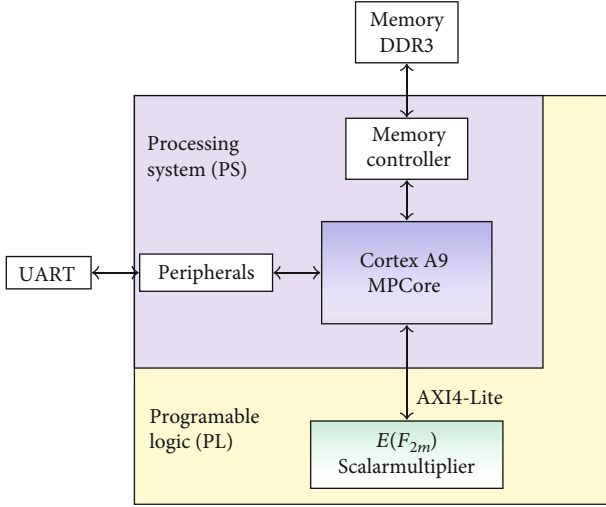


FIGURE 5: Hardware-software codesign for an FPGA-based sensor node enabled with scalar multiplier engine for curve-based cryptography.

TABLE 3: ECDH hw-sw codesign in the MicroZed board (z7010).

Size	k	Area (slices)	Freq. (MHz)	Time (ms)	MIRACL (sw) (ms)
233	32	1809	62.5	4.13	70

exchange versus the pure software implementation in the MicroZed with the MIRACL library that requires 70 ms. Thus, our codesign is 17 times faster than the pure software implementation while only requires 36% of the FPGA slices in the MicroZed, leaving 66% of the FPGA's standard logic available for other application requirements in the sensor node. These results show that our design retains the advantages of a hardware implementation by improving the performance at the time that it uses less area resources.

3.2. Comparison with Other Similar FPGA Designs. Table 4 shows a comparison with state-of-the-art works for FPGA scalar multipliers in $E(\mathbb{F}_{2^m})$. In this comparison, we are using the same elliptic curves, finite fields and sizes, and the same irreducible polynomial. A fair comparison is very difficult to achieve due to different FPGA technologies and implementation strategies being used. It is not possible to compare all the works under the same criteria, since some hardware designs exploit the use of embedded blocks such as DSPs or block rams (BRAMs) while others take advantage of the available slices/LUTs. However, this research is focused in lightweight implementations with the goal to use low standard logic resources. So, embedded memory blocks in the FPGAs are exploited to reduce standard reconfigurable logic (slices). The comparison in Table 4 is mainly in terms of FPGA standard logic (slices) reported. Although efficiency and throughput are not the main aims of this research, they are used as reference metrics.

The results presented in [32] are proposed for a digit-serial approach for multiplication and inversion over \mathbb{F}_{2^m} ,

and square and addition over $E(\mathbb{F}_{2^m})$ are computed fully with standard logic in only one clock cycle. Compared to our design, those results are almost ten times better according to efficiency. However, our design uses considerable less area resources. For example, for a digit size of 8, 16, and 32, the required area is 442, 626, and 1170 slices, respectively. In [37], it is presented a hardware architecture for elliptic curve scalar multiplication over $E(\mathbb{F}_{2^m})$ implemented for the NIST-recommended binary fields $\mathbb{F}_{2^{233}}$ and $\mathbb{F}_{2^{283}}$. That scalar multiplier hardware architecture requires 3016 and 4625 slices for the operand size 233 and 283, respectively. Compared to that design, our kP engine for $\mathbb{F}_{2^{233}}$ requires 6.8 times more slices and 2.2 times better efficiency (Mbps/slice). The scalar multiplier over $E(\mathbb{F}_{2^m})$ presented in [38] is better in efficiency than ours, but at a considerable high costs in terms of area usage.

Table 4 shows that most of the works achieve better throughput/efficiency than our proposed hardware design. However, the main aim of these works is to save hardware resources (slices), and this is achieved by sacrificing throughput. According to the obtained results, it is observed that despite the throughput sacrificing, the proposed design achieves significantly better performance than software counterparts while using fewer resources that are similar FPGA designs. The reduction in area resources is a direct result of using a digit-by-digit computing approach in the layered structure of the kP engine, mainly determined by the \mathbb{F}_{2^m} multiplier and the strategy for reusing memory blocks during the iterative processing of operands.

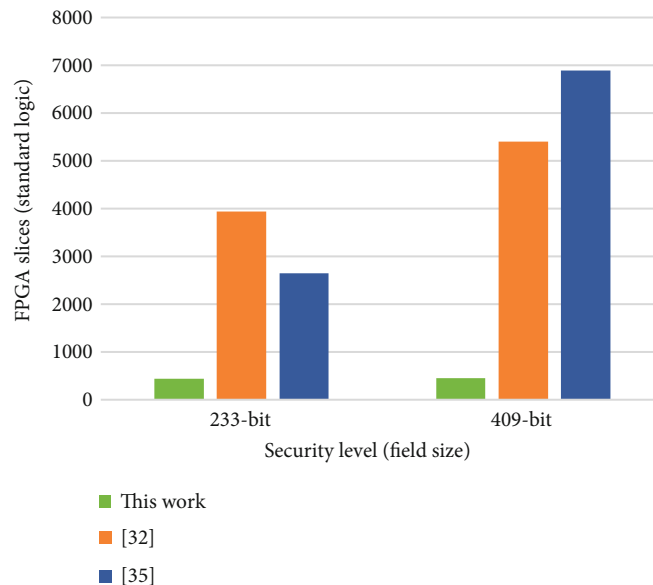
In Figure 6, we show graphically how our design uses considerable fewer standard logic resources from the FPGA, so leaving more logic for other tasks in the upper application layers. In that figure, FPGA resource usage is compared against the works that use FPGA implementation technology, digit-serial approach, and comparable security levels. Note from this figure that our design is scalable in terms of area because a greater security level only impacts latency. This property is only kept with the digit-digit computing approach.

4. Conclusion

We have detailed the design and evaluation of a compact FPGA-based ECC hardware design, well suited for Internet of Things applications, specifically for the Industrial Internet of Things (IIoT) or Internet of Medical Things (MIoT), where sensor nodes can be realized with FPGA technology. The key contributions include a novel digit-digit algorithm for multiplication over \mathbb{F}_{2^m} optimized for fields defined by trinomials and its corresponding compact hardware architecture, which is the main core for constructing a compact hardware design for computing scalar multiplications in binary elliptic curves over \mathbb{F}_{2^m} generated by trinomials, such as the ones recommended by NIST for practical use. We proposed a novel rescheduling of \mathbb{F}_{2^m} operations in the Lopez-Dahab Montgomery algorithm for elliptic curve scalar multiplication that can be computed with only two multipliers and one adder in a digit-digit fashion, thus reducing area requirements for the hardware design. For correctness, we validate our design by a hardware software codesign in the IoT

TABLE 4: Comparison of scalar multiplication over $E(\mathbb{F}_{2^m})$.

Work	FPGA	m	Cycles	Slices	Freq. (MHz)	Thrg. (kbps)	Efficiency (kbps/slice)
Prop. ($k = 8$)	z7010	233	1553782	442	190.04	28.49	0.064
Prop. ($k = 16$)	z7010	233	408547	626	149.20	85.09	0.136
Prop. ($k = 32$)	z7010	233	128820	1170	135.31	244.75	0.209
Prop. ($k = 8$)	z7010	409	7504232	453	190.94	10.40	0.023
Prop. ($k = 16$)	z7010	409	1926426	653	154.44	32.78	0.050
Prop. ($k = 32$)	z7010	409	511493	1183	132.59	106.02	0.090
[32] ($g = 16, d = 2$)	v5	233	8193	3939	263.15	7483.69	1.899
[32] ($g = 8, d = 1$)	v5	409	45513	5395	181.81	1633.82	0.030
[37]	k7	233	679776	3016	255.66	87.63	0.029
[37]	k7	283	1395312	4625	251.98	51.10	0.011
[38]	v7	233	5929	2647	370.00	14540.39	5.498
[38]	v7	409	10354	6888	316.00	12482.51	1.812
[41]	v5	163	1396	3513	147.00	17.16	0.004

FIGURE 6: Comparison of area usage for the proposed kP engine.

MicroZed Xilinx FPGA, by executing an instance of the Diffie-Hellman key exchange protocol (ECDH), a common crucial operation in IoT secure sensor nodes networks. To our knowledge, the proposed hardware ECC architecture requires less standard hardware resources (slices) in FPGAs than other works reported to date while takes advantage of memory blocks already available in modern FPGAs. Furthermore, despite of being a compact hardware architecture, it was demonstrated that a considerable acceleration of a representative curve-based cryptographic protocol is obtained compared to a pure software implementation.

Using the proposed ECC accelerator, further work is planned to evaluate the security service costs when implementing ECC-based cryptographic protocols such as digital envelopes and digital signatures in real application scenarios of IoT, IIoT, and MIIoT.

Data Availability

Raw data were generated at INAOE Computer Science Department and at Cinvestav Tamaulipas. Derived data supporting the findings of this study are available from the corresponding author MMS on request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the Fondo Sectorial de Investigación para la Educación, Ciencia Básica SEP-CONACyT,

project number 281565. Also, the research was partially funded by project PN-2017-5814, Conacyt Problemas Nacionales.

References

- [1] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.
- [2] L. Z. Cai and M. F. Zuhairi, "Security challenges for open embedded systems," in *Engineering Technology and Technopreneurship (ICE2T), 2017 International Conference on*, pp. 1–6, Kuala Lumpur, Malaysia, 2017.
- [3] D. Schinianakis, "Alternative security options in the 5g and iot era," *IEEE Circuits and Systems Magazine*, vol. 17, no. 4, pp. 6–28, 2017.
- [4] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007.
- [5] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems – a comparative analysis," *Data Privacy Management and Autonomous Spontaneous Security*, 2014, pp. 333–349, Springer, Berlin Heidelberg, 2014.
- [6] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: a survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018.
- [7] P. Yalla and J. P. Kaps, "Lightweight cryptography for fpgas," in *2009 International Conference on Reconfigurable Computing and FPGAs*, pp. 225–230, Quintana Roo, Mexico, 2009.
- [8] A. Diaz-Perez, M. Morales-Sandoval, and C. Lara-Nino, "Use of FPGAs for enabling security and privacy in the IoT: features and case studies," in *FPGA Algorithms and Applications for the Internet of Things*, chapter 2, P. Sharma and R. Nair, Eds., pp. 26–45, IGI Global, 2020.
- [9] G. Xu, Z. Chen, and P. Schaumont, "Energy and performance evaluation of an fpga-based soc platform with aes and present coprocessors," in *Embedded Computer Systems: Architectures, Modeling, and Simulation*, M. Berekovic, N. Dimopoulos, and S. Wong, Eds., pp. 106–115, Springer, Berlin, Heidelberg, 2008.
- [10] H. Abdelkrim, S. Ben Othman, and S. Ben Saoud, "Reconfigurable soc fpga based: Overview and trends," in *2017 International Conference on Advanced Systems and Electric Technologies*, pp. 378–383, Hammamet, Tunisia, 2017.
- [11] X. Zhang, A. Ramachandran, C. Zhuge et al., "Machine learning on fpgas to face the iot revolution," in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 894–901, Irvine, CA, USA, 2017.
- [12] C. Hao, X. Zhang, Y. Li et al., "Fpga/dnn co-design: an efficient design methodology for iot intelligence on the edge," in *Proceedings of the 56th Annual Design Automation Conference 2019, DAC '19*, New York, NY, USA, 2019.
- [13] S. Wang, Y. Hou, F. Gao, and X. Ji, "A novel iot access architecture for vehicle monitoring system," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 639–642, Reston, VA, USA, 2016.
- [14] B. Zhou, M. Egele, and A. Joshi, "High-performance low-energy implementation of cryptographic algorithms on a programmable soc for iot devices," in *2017 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. 1–6, Waltham, MA, USA, 2017.
- [15] Xilinx Inc, *Microzed industrial iot starter kit* April 2020, <http://zedboard.org/product/microzed-iiot-starter-kit>.
- [16] V. S. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology—CRYPTO '85 Proceedings*, H. C. Williams, Ed., pp. 417–426, Springer, Berlin, Heidelberg, 1986.
- [17] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
- [18] P. Szczechowiak and M. Collier, "Tinyibe: identity-based encryption for heterogeneous sensor networks," in *2009 International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 319–354, Melbourne, VIC, Australia, 2009.
- [19] N. Oualha and K. T. Nguyen, "Lightweight attribute-based encryption for the internet of things," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6, Waikoloa, HI, USA, 2016.
- [20] Z. U. A. Khan and M. Benaissa, "High-speed and low-latency ecc processor implementation over $gf(2^m)$ on fpga," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 1, pp. 165–176, 2017.
- [21] J. López and R. Dahab, "Fast multiplication on elliptic curves over $gf(2^m)$ without precomputation," *Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems, CHES'99*, pp. 316–327, Springer-Verlag, London, UK, UK, 1999.
- [22] D. Karaklajic, J. Fan, J. Schmidt, and I. Verbauwhede, "Low-cost fault detection method for ecc using montgomery powering ladder," *2011 Design, Automation Test in Europe*, pp. 1–6, 2011.
- [23] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov, "Triathlon of lightweight block ciphers for the internet of things," *Journal of Cryptographic Engineering*, vol. 9, pp. 1–20, 2015.
- [24] J.-L. Beuchat, T. Miyoshi, Y. Oyama, and E. Okamoto, "Multiplication over $F_{p,m}$ on fpga: A survey," in *Reconfigurable Computing: Architectures, Tools and Applications*, P. C. Diniz, E. Marques, K. Bertels, M. M. Fernandes, and J. M. P. Cardoso, Eds., pp. 214–225, Springer, Berlin, Heidelberg, 2007.
- [25] G. Bertoni, J. Guajardo, S. Kumar, G. Orlando, C. Paar, and T. Wollinger, "Efficient $GF(p^m)$ arithmetic architectures for cryptographic applications," in *Topics in Cryptology — CT-RSA 2003*, M. Joye, Ed., pp. 158–175, Springer, Berlin, Heidelberg, 2003.
- [26] C. Shu, S. Kwon, and K. Gaj, "Fpga accelerated tate pairing based cryptosystems over binary fields," *2006 IEEE International Conference on Field Programmable Technology*, 2006, pp. 173–180, Bangkok, Thailand, 2006.
- [27] L. Song and K. K. Parhi, "Low-energy digit-serial/parallel finite field multipliers," *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 19, no. 2, pp. 149–166, 1998.
- [28] D. Pamula and E. Hrynkiewicz, "Area-speed efficient modular architecture for $GF(2^m)$ multipliers dedicated for cryptographic applications," in *2013 IEEE 16th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS)*, pp. 30–35, Karlovy Vary, Czech Republic, 2013.
- [29] National Institute of Standards and Technology, *Digital Signature Standard (DSS), Appendix D, Recommended Elliptic Curves for Federal Government Use*, 1999, <https://csrc.nist>

- .gov/csrfc/media/publications/fips/186/3/archive/2009-06-25/documents/fips_186-3.pdf.
- [30] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
 - [31] D. Pamula, *Arithmetic operators on $GF(2^m)$ for cryptographic applications: performance - power consumption - security tradeoffs*, [Ph.D. thesis], Université Rennes 1, 2012, <https://tel.archivesouvertes.fr/tel-00767537>.
 - [32] G. D. Sutter, J. Deschamps, and J. L. Imana, "Efficient elliptic curve point multiplication using digit-serial binary field operations," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 1, pp. 217–225, 2013.
 - [33] A. P. Fournaris and O. Koufopavlou, "Low area elliptic curve arithmetic unit," in *2009 IEEE International Symposium on Circuits and Systems*, pp. 1397–1400, Taipei, Taiwan, 2009.
 - [34] M. Morales-Sandoval and A. Diaz-Perez, "Area/performance evaluation of digit-digit $GF(2^k)$ multipliers on fpgas," in *23rd International Conference on Field programmable Logic and Applications*, Porto, Portugal, 2013.
 - [35] I. San and A. Nuray, "Improving the computational efficiency of modular operations for embedded systems," *Journal of Systems Architecture*, vol. 60, no. 5, pp. 440–451, 2014.
 - [36] B. Bengherbia, M. O. Zmirli, A. Toubal, and A. Guessoum, "Fpga-based wireless sensor nodes for vibration monitoring system and fault diagnosis," *Measurement*, vol. 101, pp. 81–92, 2017.
 - [37] M. S. Hossain, E. Saeedi, and Y. Kong, "High-speed, area-efficient, fpga-based elliptic curve cryptographic processor over nist binary fields," in *2015 IEEE International Conference on Data Science and Data Intensive Systems*, pp. 175–181, Sydney, NSW, Australia, 2015.
 - [38] Z. Khan and M. Benaissa, "Throughput/area-efficient ecc processor using montgomery point multiplication on fpga," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 11, pp. 1078–1082, 2015.
 - [39] W. Wei, L. Zhang, and C. Chang, "A modular design of elliptic-curve point multiplication for resource constrained devices," in *2014 International Symposium on Integrated Circuits (ISIC)*, pp. 596–599, Singapore, Singapore, 2014.
 - [40] M. N. Hassan and M. Benaissa, "Low area-scalable hardware/software co-design for elliptic curve cryptography," in *2009 3rd International Conference on New Technologies, Mobility and Security*, pp. 1–5, Cairo, Egypt, 2009.
 - [41] S. S. Roy, C. Rebeiro, and D. Mukhopadhyay, "Theoretical modeling of elliptic curve scalar multiplier on lut-based fpgas for area and speed," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, no. 5, pp. 901–909, 2013.

Research Article

On the Exploitation of Blockchain for Distributed File Storage

Zuoting Ning,¹ Lijun Xiao ,² Wei Liang ,³ Weiqi Shi,¹ and Kuan-Ching Li ^{4,5}

¹Department of Information Technology, Hunan Police Academy, Changsha, Hunan, China

²Big Data Development and Research Center, Guangzhou College of Technology and Business, Guangzhou, China

³College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan, China

⁴Department of Computer Science and Information Engineering, Providence University, Taichung, Taiwan

⁵School of Computer Science and Engineering, Anhui University of Science and Technology, Huainan, China

Correspondence should be addressed to Lijun Xiao; ljxiaoxy@126.com, Wei Liang; weiliang99@hnu.edu.cn, and Kuan-Ching Li; kuancli@pu.edu.tw

Received 24 March 2020; Revised 10 July 2020; Accepted 19 August 2020; Published 15 December 2020

Academic Editor: Fei Yu

Copyright © 2020 Zuoting Ning et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Distributed file storage aims to support credible access to data on distributed nodes. There are some application scenarios, for example, data centers, peer-to-peer (P2P) storage systems, and storage in wireless networks. Nevertheless, among these applications, data blocks are inevitably replaced and inaccessible when there exists nodes failure. As a result, data integrity and credibility is absent. To overcome such a challenge, blockchain is explored to protect the distributed data. Through analysis and evaluation, we demonstrate that blockchain advocates data integrity and credibility for distributed file storage, as well as the application of blockchain technology for distributed file storage.

1. Introduction

Distributed file storage contributes to storing data over the network by distributed storage nodes. As known, there is an emergence of a large number of applications involving large data centers and peer-to-peer storage systems [1–5]. All these applications utilize nodes over the internet to approach distributed file storing. To obtain reliable storage in networks as wireless sensor networks (WSNs), additional data recovery may be required [4, 6], especially in case of a disastrous environment [5, 7].

In these applications, data reliability demands inevitably for data redundancy. In order to simplify redundancy, replication is a very suitable form, which is commonly utilized in distributed file storage systems. In research of replication, there are various methods to approach data redundancy, while erasure coding gains better storage efficiency performance. Generally, we segment a file of size S into n parts, namely, each part is of size S/n ; after that step, we code these parts into m encoded portion by adopting (m, n) maximum distance separable code (MDSC); at last, all coded portion

are stored on M nodes. In this way, we can recover the original file from any set of n linearly independent coded parts. As a result, optimal performance can be harvested, such as better decisions for incredibility and redundancy trade-off. There are some researches utilizing erasure codes to reduce data redundancy [6–8].

At present, among many domains, such as academia and industry, they have paid attention to the distributed ledger and blockchain technology as well as its massive potential in managing complicated systems. The distributed ledger is mainly composed of a certain amount of blocks [9], chained back that utilizes a linked hash-pointer list, so data blocks store valid sequential transactions with digital assets (see Figure 1).

Nevertheless, when any data block is attacked, we cannot recover the source file, since all segmented pieces are linearly independent. In order to solve this issue, literature [8] proposed a scheme that aims to reduce computation complexity by probabilistically verifying blocks of data. Liang et al. [10] put forward a recommendation scheme to obtain data credibility. It is depicted that, by using a homomorphic signature,

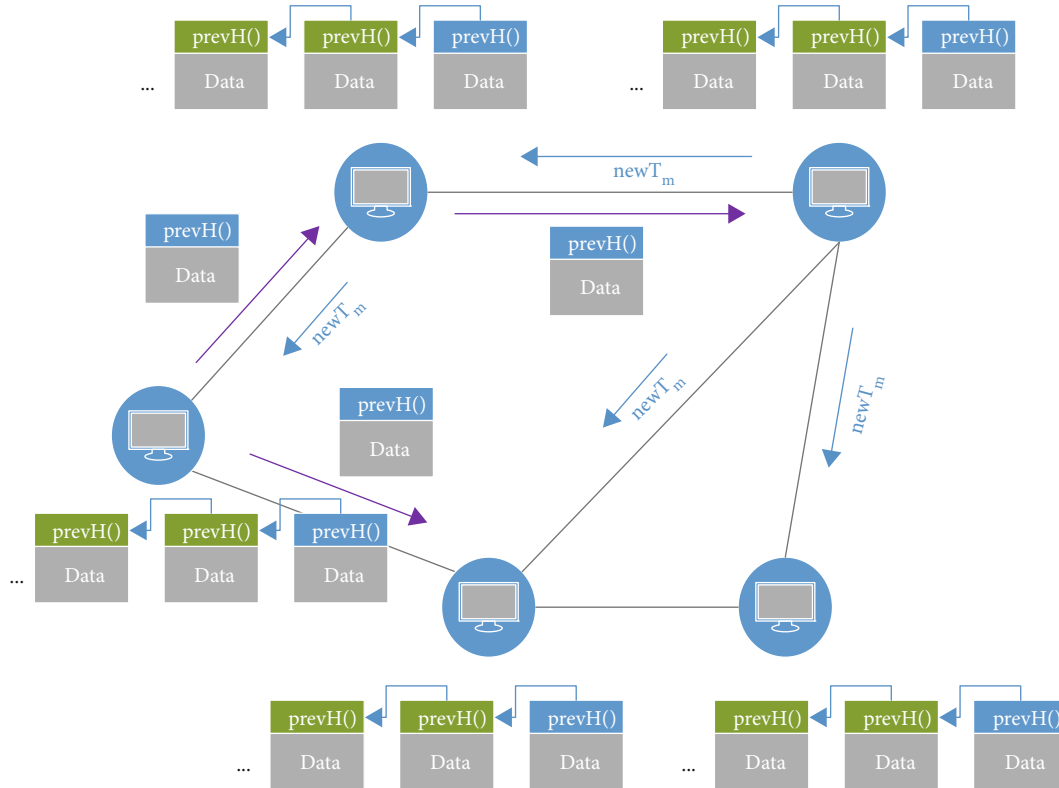


FIGURE 1: Ledger distribution in peer-to-peer network.

intranetwork verification can harvest data credibility [11, 12], a polynomial-time algorithm is applied to protect networks from malicious attacks [13], and a scheme is designed to resist pollution attacks by utilizing a polynomial hashing function [14].

In this paper, in order to conquer data integrity and incredibility issues, we utilize a blockchain-based approach for distributed file storage. The main contribution of this paper is the following: firstly, we utilized distributed hash table to enhance the credibility for stored files; secondly, we proposed a blockchain-based framework for a distributed file storage system to approach integrity and security; finally, we carried out detailed discussion on the load balance, throughput, and risk of attacks.

2. Background and Related Work

2.1. Distributed File Storage System. Nowadays, there are various types of distributed storage systems, such as cloud storage systems, and peer-to-peer (p2p) storage systems. In all these storage systems, data can be stored, archived, and back up over distributed nodes, such as AmazonS3. Users can make use of their stored files any time anywhere; this is an outstanding advantages as to distributed storage systems. There are many researches focused on the design and construction of distributed file systems. Napster [15], Kazaa [16], and Gnutella [17] implement distributed file systems and prompt it to be an exciting and popular research area. Bit-torrent [18] is one of the most popular and successful peer-to-peer distributed file systems and has more than 100

million online users presently. It is a large-scale deployed in which millions of users log-in and log-out every day. Storage resources, as well as system clients in a distributed file system, are scattered in the network. In these systems, users act as both creators and consumers of data, therefore, to provide massive of incentives by a secure and efficient approach.

Various recent studies have explored and carried out evaluations for distributed file storage systems [2, 6, 19–22]. Some literatures [2, 7, 8, 22–26] proposed and evaluated redundancy management strategies. Among these, replication and erasure codes are compared in bandwidth and reliability trade-off in literatures [2, 7, 8]. Literature [7] argues that, compared with replication, erasure codes can harvest better bandwidth performance. Literature [2] also approves this conclusion through a distributed file storage system. Based on a novel data clustering optimization model, Liang et al. put forward an intrusion detection algorithm for the industrial network [27]. A hybrid strategy is proposed in the literature [8] to conquer the repair problem. The node storing the replication can generate new pieces and then deliver them to the new users. As a result, it only transfers only S/n to a new segment. Nevertheless, supporting an extra replication decreases the bandwidth-performance; that is because when the replication is polluted or lost, new segments cannot be produced. Meanwhile, there exists support [28] for static policies to solve data block replications. These schemes should be manually configured and primarily focus on archival purposes [29], by utilizing disk caching, MixA-part [30], and Rhea [31] research data retrieval. What is more, literature [30] schedules tasks by using remote data

and local caching, while static analysis strategy to harvest storage performance is utilized [31]. Liang et al. [32] put forward an efficient protocol to approach identity authentication in the IoT environment.

2.2. Blockchain. The blockchain technology is a chain of blocks based on time-stamp that is jointly sustained by each on-chain node. Every block acts as a container role aggregating all on-chain transactions and chained by cryptography technology. That is, each participating block is chained together and signed by their private secret key as well as their respective hash value. Once a new block is created, this new block will be chained together. In this way, the blockchain provides a steady data storage, so any deletion or update on processed transactions is impracticable [33]. Due to this characteristic, we can make full use of this advantage in the proposed work. In other words, all transactions are reliable without a third-party authority. The advantage of blockchain resists all stored data from repudiation. Moreover, user identity and authenticity are guaranteed by cryptography and digital signatures, so thus any illegal read or write will be refused over the blockchain.

Bitcoin, which is regarded as the first practice of the blockchains, is a public distributed ledger; it plays an essential role in promoting blockchain. After that, smart contracts [34] emerged, which is an autonomous program deployed on the blockchain network and makes all transactions intelligently. In the practice of blockchain, smart contracts act the role of triggers [35]. For example, based on the smart contract, all services will not hold funds unless all tasks in the contract have been finished. According to this theory, Ethereum regards and promotes the smart contract to the top level. Nowadays, blockchain has turned to be a promising topic in both industry and academy area, and combining blockchain and distributed file system becomes an exciting and promising solution, in which blockchain provides incentives and security for distributed files. Up to now, the popular and famous distributed file systems are IPDFS [36], Storc [37], Swarmer [38], and PPIO [32]. In these systems, IPDFS is a peer-to-peer distributed file system that is used to store and access files, applications, websites, and data; Storc is another peer-to-peer decentralized cloud storage platform allowing users to share data and has no need of any third-party data provider; Swarmer, based on Ether, is a distributed storage platform and content-distributed service, and PPIO that permits users to store and retrieve data on web anywhere and anytime is a programmable distributed storage network.

With the introduction of the blockchain, three distributed file systems utilize File-coin [39], Ether [40], and Meta-disk [41] as correspondingly stimulative mechanisms. Based on the industrial blockchain network environment, Liang et al. proposed secure data storage and recovery strategy [3], while Zhang et al. utilize the blockchain to improve 5G performance [42].

3. Problem Statement

Due to issues in integrity, trust, control, and credibility, we focus in this paper on overcoming the issue of integrity and

credibility for distributed file storage. There are various systems and platforms for distributed file storage, and they aim to collect all kinds of data. Notably, this incurs a severe privacy problem, since most users have no knowledge of these actions, much less about control of such actions. To solve this problem, we suppose in this work that all provided services should obey the smart contracts, especially some assigned protocols. Based on this, this proposed work devotes to the following issues:

Data Credibility. Our research focuses on the data credibility for distributed file storage; we should guarantee that authorized users must control all personal data. Meanwhile, the systems and platforms regard the services as guests who have corresponding permissions.

Data Integrity. All data should be verified and detected to guarantee the integrity of stored data. All data-trace is totally transparent for each authorized user, and any illegal modification is impractical on the platform.

Access Control. Any users should be granted access permission as they log in the system or platform. These permissions should define which resources the users can utilize. Within the permissions, users can change the access range of their stored data. Meanwhile, all participating users must store data access control strategies or policies on the blockchain. Thus, illegal access is hardly impossible.

4. Our Solution

4.1. Distributed System. In this paper, we design a decentralized system. There are mainly three parts comprising the system: nodes, users, and services, as shown in Figure 2. Users can store and utilize their corresponding distributed files, as all operations on distributed data are supported by the services; the nodes play an essential role as storing users' distributed files encrypted with their private keys. In order to simplify user authentication, we produce message digest for each stored file on the chain. In the proposed system, blockchain is very critical, since it only accepts two kinds of data, namely, G_{access} and T_{data} . The former is utilized for access control, while the latter is used for user data storage or data retrieval. The two types of operations can be arranged on the SDK (Software Development Kit), and users can use them through complete services.

To describe the proposed system in details, we assume the following application service: when a user intends to store files on the proposed system, he will first install the system application. The user signs up on the proposed system, and the system will generate an identity for the user, so then this identity will be informed to the blockchain, as well as the user's permissions. The user's files will be segmented into pieces and then encrypted by their shared keys. After that, all segmented files are stored on the nodes in a distributed way. In the meanwhile, all encrypted files are sent to the chain with T_{data} , and a special pointer produced by the hash of segmented files to the blockchain is maintained.

When users issue data query requests, they can use T_{data} together with the aforementioned unique pointer. Once the blockchain receives this request, it will check the identity of the users by verifying users' digital signature. Only when

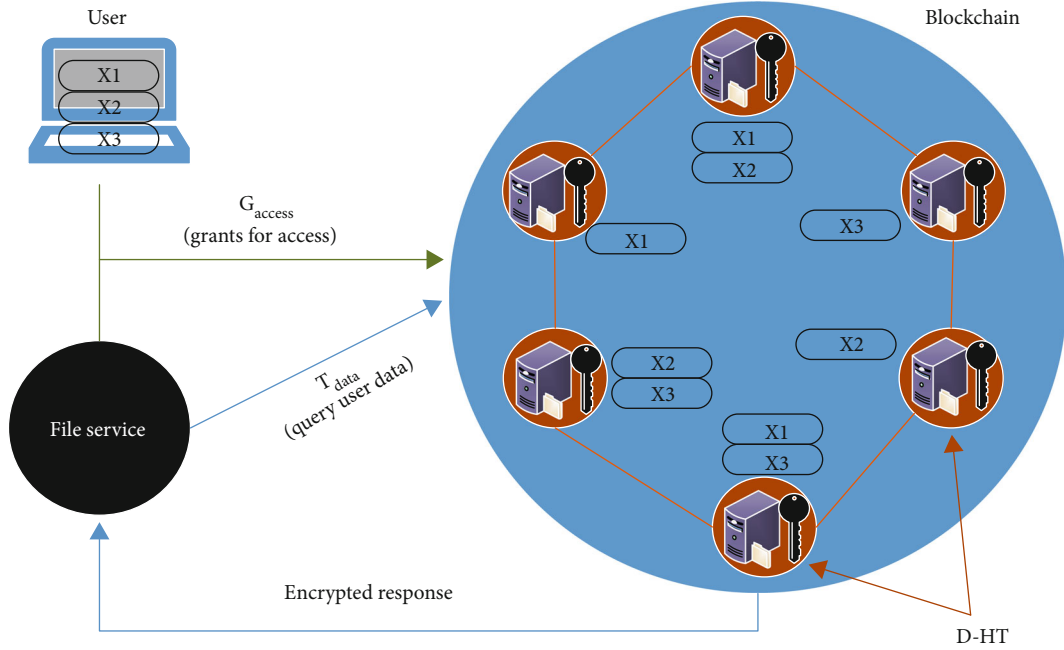


FIGURE 2: System framework.

the users have passed verification, they can carry out the operation within their authorized permission. They can have an overview of their file data and modify corresponding permissions. All these operations are recorded in the blockchain. We utilized D-HT (Distributed Hash Table) to carry out a key-value store for off-blockchain in this implementation, and it interacts with the blockchain through an interface. During the processing, the D-HT is utilized by the nodes on the chain, so any general operations, such as read and write, shall be approved by D-HT, and thus, users' files can be of high availability.

4.2. Building Blocks. In this subsection, to approach the proposed solution, a detailed description of how to building the blocks follows next. Accordingly, the process of building blocks follows Bitcoin [43].

- (1) **Identities.** To identify users, we utilize a pseudo-identity scheme. That is, each user on the chain can produce pseudo-identity by their public keys, and the practical requirements determine the number of pseudo-identities, which can critically improve the user's privacy. In this work, we explore compound identities that are originated from the existing theory. As there may be more than two participators during transactions, some participators can hold this compound identity, though the remaining have no permissions to use it. As depicted in protocol one, we assume there are only one owner and one guest, and this protocol describes how we implement this operation. To guarantee the credibility, we utilize asymmetric key pairs to authorize user's identity, as to encrypt or decrypt the user's distributed files, we use asymmetric key that can promote the efficiency

of encryption and decryption. In this way, all data are secure for each one of the users. The compound identity is defined as the following:

$$Compound_{o,g}^{public} = (pk_{sig}^{o,g}, sk_{sig}^{o,g}). \quad (1)$$

As to the whole identity, we formulate it as a 5-tuple:

$$Compound_{o,g} = (pk_{sig}^{o,g}, sk_{sig}^{o,g}, pk_{sig}^{g,o}, sk_{sig}^{g,o}, sk_{enc}^{o,g}). \quad (2)$$

- (2) **Policy.** In this paper, we define a group of permissions, which a data owner o grants a guest g , as $POLICY_{o,g}$. Supposing the following scenarios, if the owner o deploys an application that calls for access to o 's location or contacts, this can be denoted as, $POLICY_{o,g} = o_{location}, o_{contacts}$. It describes that all types of data should be stored according to this way, supposing the service does not tear up the protocol and error-mark the data, then safeguards, which are utilized to avoid this, should be preferentially recommended to SDK. Moreover, according to this method, every user can quickly verify the legality of service, since any change is fully visible
- (3) **Auxiliary Functions.** In the function $ChkPolicy(pk_{sig}^{sk}, m_p)$, $Parse(m)$ de-serializes these messages that are delivered to a general transaction containing the arguments $ChkPolicy(pk_{sig}^{sk}, m_p)$, as is described in the protocol two. This function validates whether

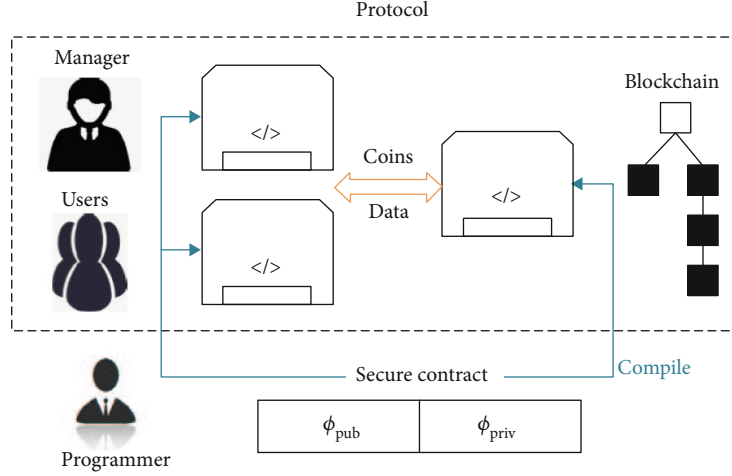


FIGURE 3: Smart secure contract.

the initiator has relevant permissions, which can guarantee the validity of each operation

Protocol 1: Compound identity description.

- 1: Procedure CompoundIdentity(o, g)
- 2: o and g compose of a secure channel
- 3: u executes:
- 4: $(pk_{sig}^{o,g}, sk_{sig}^{o,g}) \leftarrow O_{sig}()$
- 5: $sk_{enc}^{o,g} \leftarrow O_{enc}()$
- 6: u shares $sk_{enc}^{o,g}, pk_{sig}^{o,g}$ with s
- 7: s executes:
- 8: $(pk_{sig}^{g,o}, sk_{sig}^{g,o}) \leftarrow O_{sig}()$
- 9: g shares $pk_{sig}^{g,o}$ with o
- 10:// Both o and g have $sk_{enc}^{o,g}, pk_{sig}^{o,g}, pk_{sig}^{g,o}$
- 11: Return $pk_{sig}^{o,g}, pk_{sig}^{g,o}, pk_{sig}^{o,g}$
- 12: end Procedure

Protocol 2: Verify permission.

- 1: Procedure: ChkPolicy(pk_{sig}^{sk}, m_p)
- 2: $g \leftarrow 0$.
- 3: $a_{policy} = H(pk_{sig}^{sk})$
- 4: if $L[a_{policy} \neq \varphi]$ then
- 5: $pk_{sig}^{o,g}, pk_{sig}^{g,o}, POLICY_{o,g} \leftarrow Execute(L[a_{policy}])$
- 6: if $pk_{sig}^{sk} = pk_{sig}^{o,g}$ or
- 7: $(pk_{sig}^{sk} = pk_{sig}^{g,o} \text{ and } m_p \in POLICY_{o,g})$ then
- 8: $g \leftarrow 1$.
- 9: endif
- 10: endif
- 11: return s
- 12: end Procedure

In order to guarantee the validity of each operation, we create a checking-policy function $ChkPolicy(pk_{sig}^{sk}, m_p)$ to

verify permission, which simplifies the access verification compared with these existing approaches [22, 35, 39].

4.3. Smart Secure Contracts. In this section, we explore a blockchain-based framework for a distributed file storage system to approach security. As depicted in Figure 3, the framework is composed of two parts:

- (1) In contracts, it contains each user's operation data, including variate $\varphi_{private}$ that denotes user's private data that carries out computation for distributed data. Suppose the following scenario that, during an open auction, only the winner's final bids approach to the seller, and the other bids are totally refused. Thus, variate $\varphi_{private}$ guarantees the security for users' distributed data
- (2) Variate φ_{public} , which has no user's private data, denotes users' public data. Meanwhile, we define the cryptography protocol that is used during the transaction on the chain

Security guarantees. Security guarantees mainly include the following aspects:

- (i) Chain-to-Chain Privacy. Chain-to-chain privacy indicates that the user's distributed file or data should be protected against any users not included on the blockchain, only if the legal users intend to inform others of their information. In our proposed protocols, all users should interchange data and depend on blockchain to guarantee fairness. That is, all users transmit their encrypted files or data to the chain, what is more, as also all transactions are based on zero-knowledge authorization
- (ii) Security. As chain-to-chain privacy prevents the user's data from the public chain, all users' data are entirely independent of each other. Meanwhile, asymmetric encryption guarantees the authenticity


```

1:Declare Member(Seller/* M parties */)
2:Declare Timeouts(/* timeouts */)
3:Declare Function contract auction(In &input, Out &output)
4:Set win = -1
5:Set btpri ce = -1
6:Set sec dprice = -1
7:loop
8:  for each j < m do
9:    if input.pat[j].value > btpri ce then
10:     Let sec dprice = btpri ce
11:     Let btpri ce = input.pat[j]
12:     Let winner = j
13:  else if input.pat[j].value > sec dprice then
14:    Let sec dprice = input.pat[j].value
15://The winner pays the bidder
16://The others are refused
17:Let output.seller.value = sec dprice
18:Let output.pat[win].value = btpri ce - sec dprice
19:Let output.win = win
20:for each j < m do
21:  if j ≠ win then
22:    output.pat[j].value = input.pat[j].value

```

ALGORITHM 1: Process for public auction.

and confidentiality. We take a public auction as an example to describe the security of the scheme. The above Algorithm 1 shows the process of a public auction. In this example, auction transaction contains φ_{private} , which indicates that who wins the bidder and how much he should pay. Meanwhile, variate φ_{public} , which depends on the deposits, is used to avoid the winners from abandoning

An auction is of the abovementioned specified requirements, especially in terms of security and confidentiality, and this is accomplished by cryptocurrency, as present in some existing systems [44, 45]. The program, as depicted in the algorithm, declares timeout parameters. The timeout parameters are declared as $P1 < P2 < P3$. P1: the contract stops receiving bids after P1. P2: the bidder should tell the price within time P2; otherwise, its input bid is regarded as 0. By doing this, the auction transaction continues. P3: supposing the auction manager abandons the bid, bidders may withdraw their bids when time P3 elapses.

Variate φ_{public} plays an essential role in the auction transaction. As it not only checks the time but also manage the timeout. The system will invoke the function only if the operation completes within P3. Otherwise, the system will invoke the manager's TimeOut function.

5. Theoretical Analysis

5.1. Credibility. In a blockchain system, it supposed that all nodes should be untrustworthy. That is, every node should be verified. Moreover, nodes' resources for computing determine their credibility level [43]. For example, a node m , $m \propto$ resources (m) denotes that how much weight node m votes,

which means that wither the node is vulnerable when there is high energy consumption, or there is high latency of a transaction.

In this paper, as to formulate the value for all nodes' trust, we compute each data block b of a node like the following:

$$rely_t_m^{(b)} = \frac{1}{1 + e^{(-\beta)(\#legitimate-illegitimate)}}, \quad (3)$$

in which the step size is defined by β .

In the above equation, it is regarded that these nodes on-chain has higher weight as well as more efficiency in computation. Due to this reason, these nodes have the ability to resist fraud attacks.

5.2. Risk of Attack. In a blockchain, there is the risk of fraud, but this is complex, because it should approach 51%, the risk occurs. However, the risk exists, although hardly impossible to reach such a high percent of nodes failure. The current public blockchain structure is vulnerable to some particular scenarios: the software update, blockchain entry changes, as an example. This is due to, when all transactions are processing, any new participators can have knowledge of the decisions of the network. As to the network, based on its majority rules, 51% of undergoing transactions could do any operation on the chain.

51% attack on the chain may sharply increase the vulnerability, as there may exist fork attack. This is because more than two networks share the resources of a single network, leading to a quick decrease in computation ability. Namely, the cost of launch attack on the networks is lower, and cause to a growing risks for the network.

The probability that an attack chain can catch up with the honest chain is shown in the following equation.

$$q_z = \begin{cases} 1, p \leq q \\ (q/p)^z, p > q \end{cases}. \quad (4)$$

p represents the probability that honest miners find the next block, q is the probability that attackers find the next block, and q_z is the probability that attackers change the trading content of the current blocks.

5.3. Load Balance. In our research, load balancing is an important index. We are aiming at distributing all requests efficiently on each node, and this can harvest great improvement in load balancing. In this paper, any nodes act the role of sustaining as many online I/O connections as possible; we use variate ($NumAct[s_j]$) to represent the number of connections, while variate s_j denotes storage media. These two variables should be stored to the nodes within any transactions, correspondingly. Generally, the more the number of connections to the storage media, the lower the proportional of the throughput of the nodes. That is, if we intend to approach the better performance of load balancing, the participating nodes should have fewer connections. For ease of description, we introduce function f_{ub} , and formulate the load balancing as the following:

$$f_{ub}(\vec{s}) = \sum_{s_j \in \vec{s}} \left(\frac{1}{NumAct[s_j] + 1} \right). \quad (5)$$

Where function f_{ub} approaches maximum when all storing nodes have the lest count of active connections. Function f_{ub} approaches to the upper bound when the very lest connecting number occurs. This is an exciting discovery for each storage media. As a result, we can optimize the function f_{ub} and harvest the following formulation:

$$f_{ub}^*(\vec{s}) = \left| \vec{s} \right| \times \frac{1}{\min_{s_j} (NumAct[s_j] + 1)}. \quad (6)$$

5.4. Throughput. As to distributed file storage systems, we devote to harvest best throughput performance. We store data in the manner of tiers, so thus, we can make full use of fast storage characteristics of tiers, which helps harvest optimized throughput. Once there is a request, the system will check the ability level for reading and write throughput of storing node $node_i$ by a quick I/O test, and the read and write throughput is denoted as $ReadTh[node_i]$, $WriteTh[node_i]$, respectively. After that, we calculate the average value and store them on the node.

To approach the maximum throughput, any operation for distributed file storage is of the optimal write or read throughput. Generally, to obtain the common value, we regard the proportional peak value of nodes' throughput as the final value. Moreover, in order to scale the throughput down, we introduce the logarithm function for these throughput values.

TABLE 1: Theoretical results.

	Declare-or-refuse [46]	Multiple lock [47]	Blockchain
Chain-to-chain cost	$O(P^2)$	$O(P^2)$	$O(P)$
Amount of rounds	$O(P)$	$O(1)$	$O(1)$

Similarly, we formulate the throughput function f_{tm} as:

$$f_{tm}(\vec{node}) = \sum_{node_i \in \vec{node}} \left(\frac{\log(WriteTh[node_i])}{\log(\max_{node} WriteTh[node])} \right). \quad (7)$$

As to the storage nodes, by computing function f_{tm} , we retrieve the throughput for storage node, when a specified number of nodes with the optimal throughput are on the chain. Once there are always many nodes with optimal throughput, the function approaches the upper bound. Therefore, we can optimize the function f_{tm}^* and formulate it as:

$$f_{tm}^*(\vec{node}) = \left| \vec{node} \right|. \quad (8)$$

5.5. Theoretical Results. In Table 1, we assume that there are P participators who intend to calculate a one-bit outcome and send it to all P participators. We made comparisons among literature [46, 47], and blockchain, and we conclude that blockchain is most useful for distributed file storage. Public storage in the blockchain-based system was first approved in the literature [48]. Fairness can hardly be impractical in general models for multiparticipator transactions, which is proposed in the literatures [49, 50]. Base on the script language, some works about construct abstractions for protocols emerge, for example, "Declare-or-refuse" [46] or "multiple locks" [47].

5.6. Blockchain Application Systems. Table 2 shows four blockchain-based application systems, and we make a comparison in terms of blockchain form, protocol, cryptocurrency, and intelligent contracts. Super-ledger [51], which is an open-source system based on blockchain, was developed to improve the efficiency of distributed file storage. It was developed by superior language and supported any application on the chain, and meanwhile, it supported distributed components and maintained membership.

The multiple chain [52] system aims to create the private key for users, as well as deploy the blockchain. It depends on the API to expand the core API, which permits managing all transactions, assets, and resources. This system has good operability for users to interact with networks, such as users can directly utilize command tools, and distributed clients can carry out transactions with the network by JSON, especially Ruby, Node.js, and Cij. This characteristic makes this system have excellent convenience of operation.

TABLE 2: Blockchain application systems.

System	Blockchain	Agreement	Crypto currency	Intelligent contracts
Super-ledger	Based on permission	SIEVE	No	Yes
Multiple chain	Based on permission	PBTF	Multiple currencies	Yes
ETH	Public chain	PoS	Ether	Yes
LTC	Public chain	Scrypt	LTC	No

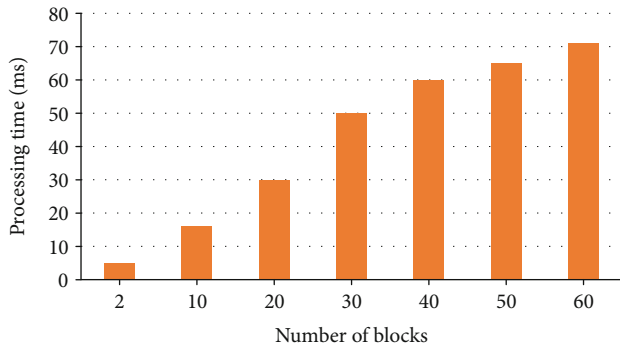


FIGURE 4: Processing time overhead.

As one of the many systems, ETH [53] is very popular with distributed file storage for nowadays, especially on its excellent advantage of smart contracts in blockchain. This platform can both run on fysieke computer and virtual machine, meanwhile, and it can be programmed with general procedure language. Therefore, it is an exciting platform for users in distributed file storage.

LTC [54], which is illustrated in Table 2, is a public chain-based technology for the distributed file storage system. It has very distinct features, such as fast speed for all transactions and marvelous efficiency for file storage. As its all transactions are executed in intensive memory, it needs very fewer nodes to participate computations, even though its transactions are encrypted and signed either by symmetric or asymmetric manners.

From Table 2, we can conclude that, in most systems, there are fewer smart contracts, which might cause risks for blockchain application. In this system, when a user deploys blockchain, there is a trade-off on cryptocurrency and blockchain. Moreover, this system is capable of supporting all applications based on blockchain. Users can assemble their own infrastructure, just like some popular cloud platforms, such as Amazon and Google.

6. Experiment and Evaluation

6.1. Experimental Results. The evaluation is executed on a Windows 10 machine equipped with an Intel(R) Core(TM) i7-7700M CPU @ 3.60 GHz, 16 GB RAM. The transaction nodes have been deployed in a virtual machine which is supported with Ubuntu 16.04.

Processing time overhead refers to the time consumed by the transaction nodes to verify data blocks. The experimental results are shown in Figure 4. At first, the processing time is about 5.5 ms. As more data blocks are generated, the process-

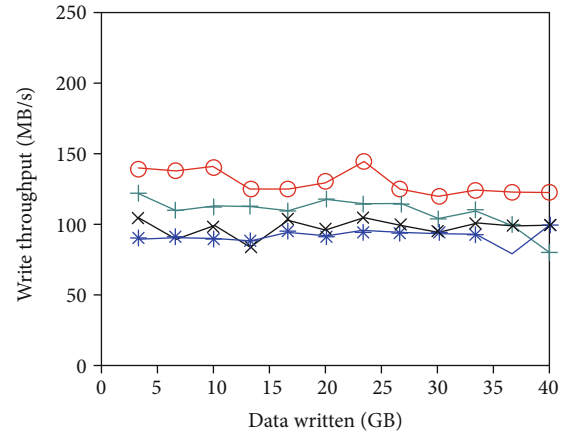


FIGURE 5: Average throughput for writing data.

ing time overhead increases; especially, there is a sharp increase of time overhead when the number of blocks changes from 20 to 30. After that, the time overhead increases smoothly. When the number of blocks comes to 60, the processing time overhead approaches about 71 ms.

6.2. Evaluation. In order to support our proposed scheme, we carried out evaluations and utilized the mostly adopted benchmarks, namely DFSIO [4], which is mainly focused on measuring network throughput for users' general operations, such as read and write. Additionally, this benchmark is based on a distributed approach.

The principal evaluation methodology is as the following: we focus on the data storing policy as well as the optimization goals, especially for data writing and reading throughput. Moreover, we make a comparison among the proposed schemes, the HDFS [4] and the rule-based strategy.

As depicted in Figure 5, the comparison result, we carry out about 20 times of evaluation and obtain the average throughput of every node for writing. The blockchain-based method gets the highest throughput, nearly about 138 MB/s, which is mainly due to the full use of its advantages, such as the optimal design of storage tier. However, the curve smoothly descends when the storage space (mainly memory) is mostly consumed, and this is a universal phenomenon for distributed file storage systems. The HDFS performs the worst, since its throughput only approaches average about 88 MB/s; this is due to the abandon of storage metrics.

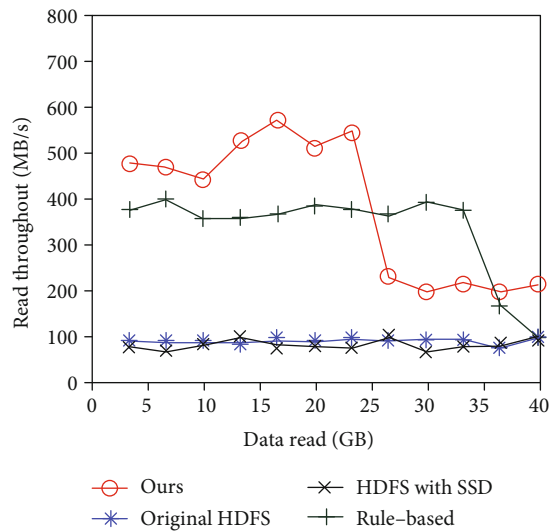


FIGURE 6: Average throughput for reading data.

Figure 6 shows the results of the READ throughput, where the HDFS strategy changes smoothly around 99 MB/s, while the HDFS with SSD policy exhibits a similar trend. While our proposed scheme harvests the best performance, the observations are twofold. As the former one, the proposed scheme equally distributes all requests onto all nodes, while the proposed scheme utilizes more HDDs storage media as the latter one. Accordingly, it can write more data blocks than the other policies. Neither the Original HDFS nor HDFS gets worse performance for reading data, respectively. Especially, HDFS yields the worst read performance.

7. Conclusion and Future Work

The distributed file storage system is susceptible to malicious use and fraud attack; users sometimes cannot have full control over their data. In this paper, we innovatively explore blockchain in distributed file storage, users no longer require a third-party, and own heavy supervision of their data. Through analysis and evaluations, our proposed scheme significantly improves data integrity and credibility for distributed file storage. Besides, based on blockchain, decisions on distributed file storage shall be more easier and reasonable. Finally, we carried out detailed discussion on the latest relative systems and demonstrated the advantages of this proposed work in distributed file storage.

As future directions, considering the network latency of the blockchain-based system, we will investigate the time tolerance of blockchain-based distributed file system and focus on the combination of network coding and blockchain to explore optimal network performance.

Data Availability

The test data, simulation data, and the proposed method used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This work is supported by the Science and Technology Projects of Hunan Province of China under Grant No. 2017SK1040, the Science Research Project of Education Department of Hunan Province under Grant No. 19B180, the Natural Science Foundation of Hunan Province under Grant No. 327 2018JJ2107, the Scientific research project of Guangzhou College of Technology and Business under Grant No. KA202031, the National Natural Science Foundation of China under Grant No. 61702180, and the Natural Science Foundation of Hunan Province under Granted No. 2019JJ50167.

References

- [1] C. Xie, Y. Sun, and H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 45–50, Chengdu, China, 2017.
- [2] T. T. Nguyen, T. K. Vu, and M. H. Nguyen, "BFC: high-performance distributed big-file cloud storage based on key-value store," in *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 1–6, Takamatsu, Japan, 2015.
- [3] W. Liang, K.-C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2063–2071, 2020.
- [4] K. Shvachko, H. Kuang, S. Radia, and R. Chansler, "The hadoop distributed file system," in *2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST)*, pp. 1–10, Incline Village, NV, USA, 2010.
- [5] A. Kamra, J. Feldman, V. Misra, and D. Rubenstein, *Growth Codes: Maximizing Sensor Network Data Persistence*, ACM SIGCOMM, 2017.
- [6] Y. Tang, F. Li, and Y. Wu, "Research on the network coding for distributed storage file system based on the wavelet support vector machine," *Journal of Computational and Theoretical Nanoscience*, vol. 13, no. 12, pp. 9628–9632, 2016.
- [7] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure fabric blockchain-based data transmission technique for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3582–3592, 2019.
- [8] J. Li, C. Pan, and M. Lu, "A seismic data processing system based on fast distributed file system," *International Journal of Computers & Technology*, vol. 14, no. 5, pp. 5779–5788, 2015.
- [9] B. Karthikeyan, A. Delignat-Lavaud, C. Fournet et al., "Formal verification of smart contracts," in *Proceedings of the ACM-Workshop on Programming Languages and Analysis for Security*, pp. 91–96, Vienna, Austria, 2016.
- [10] W. Liang, W. Huang, J. Long, K. Zhang, K.-C. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6392–6401, 2020.

- [11] D. Liao, G. Sun, G. Yang, and V. Chang, "Energy-efficient virtual content distribution network provisioning in cloud-based data centers," *Future Generation Computer Systems*, vol. 83, pp. 347–357, 2018.
- [12] Coinmarketcap, "Crypto-currency market capitalizations," 2016, <https://coinmarketcap.com/>.
- [13] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Meard, "Resilient network coding in the presence of byzantine adversaries," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pp. 616–624, Barcelona, Spain, 2007.
- [14] T. Ho, B. Leong, R. Koetter, M. Meard, M. Effros, and D. Karger, "Byzantine modification detection in multicast networks using randomized network coding," in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*, p. 144, Chicago, IL, USA, 2004.
- [15] M. Giesler and M. Pohlmann, *The Anthropology of File Sharing: Consuming Napster as a Gift*, ACR North American Advances, 2003.
- [16] N. S. Good and A. Krekelberg, "Usability and privacy: a study of kaza P2P file-sharing," in *Proceedings of the conference on Human factors in computing systems - CHI '03*, pp. 137–144, Ft. Lauderdale, FL, USA, 2003.
- [17] M. Ripeanu, "Peer-to-peer architecture case study: Gnutella network," in *Proceedings First International Conference on Peer-to-Peer Computing*, pp. 99–100, Linköping, Sweden, 2001.
- [18] J. Pouwelse, P. Garbacki, D. Epema, and H. Sips, "The bit torrent p2p file sharing system: measurements and analysis," in *Peer-to-Peer Systems IV*, pp. 205–216, Springer, 2005.
- [19] S. Wang and L. Cao, "Inferring implicit rules by learning explicit and hidden item dependency," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 3, pp. 935–946, 2020.
- [20] K. Zhang, Y. Zhu, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Deep learning empowered task offloading for Mobile edge computing in urban informatics," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7635–7647, 2019.
- [21] K. Ikeda, *qBitcoin: A Peer-to-Peer Quantum Cash System*, Social Science Electronic Publishing, 2017.
- [22] K. K. Mar, Z. Q. Hu, C. Y. Law, and M. Wang, "Secure cloud distributed file system," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 176–181, Barcelona, Spain, 2016.
- [23] D. C. M. Segura, M. D. C. Oliveira, T. K. Okada et al., "Availability in the flexible and adaptable distributed file system," in *2015 14th International Symposium on Parallel and Distributed Computing*, pp. 148–155, Limassol, Cyprus, 2015.
- [24] S. Wang, L. Hu, Y. Wang, Q. Z. Sheng, M. Orgun, and L. Cao, "Intention nets: psychology-inspired user choice behavior modeling for next-basket prediction," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 4, pp. 6259–6266, 2020.
- [25] J. Yin, J. Wang, J. Zhou, T. Lukasiewicz, and J. Zhang, "Opass: analysis and optimization of parallel data access on distributed file systems," in *2015 IEEE International Parallel and Distributed Processing Symposium*, pp. 623–632, Hyderabad, India, 2015.
- [26] K. Zhang, S. Leng, X. Peng, L. Pan, S. Maharjan, and Y. Zhang, "Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1987–1997, 2019.
- [27] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020.
- [28] A. Purtell, "Support tiered storage policies in HDFS," 2015, <https://issues.apache.org/jira/browse/HDFS-4672>.
- [29] T.-W. N. Sze, "Support archival storage in HDFS," 2015, <https://issues.apache.org/jira/browse/HDFS-6584>.
- [30] M. Mihailescu, G. Soundararajan, and C. Amza, "Mix apart: decoupled analytics for shared storage systems," in *Presented as part of the 11th {USENIX} Conference on File and Storage Technologies ({FAST} 13)*, pp. 133–146, San Jose, CA, USA, 2013.
- [31] C. Gkantsidis, D. Vytiniotis, O. Hodson, D. Narayanan, F. Dinu, and A. I. Rowstron, "Rhea: Automatic Filtering for Unstructured Cloud Storage," in *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*, pp. 343–355, Lombard, IL, USA, 2013.
- [32] W. Liang, S. Xie, J. Long, K. C. Li, D. Zhang, and K. Li, "A double PUF-based RFID identity authentication protocol in service-centric internet of things environments," *Information Sciences*, vol. 503, pp. 129–147, 2019.
- [33] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Zomaya, "Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection," *IEEE Transactions on Emerging Topics in Computing*, p. 1, 2020.
- [34] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," *AI Matters*, vol. 1, no. 2, 2014.
- [35] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in *Business Process Management. BPM 2016*, vol. 9850 of Lecture Notes in Computer Science, pp. 329–347, Springer, 2016.
- [36] J. Benet, "IpfS-content addressed, versioned, p2p file system," 2014, <https://arxiv.org/abs/1407.3561>.
- [37] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a Peer-to-Peer Cloud Storage Network," 2014, <https://storj.io/storj2014.pdf>.
- [38] V. Trón, A. Fischer, and Nagy, *State channels on swap networks: claims and obligations on and off the blockchain*, Ethersphere Orange Papers, 2016.
- [39] J. Benet and N. Greco, *Filecoin: A Decentralized Storage Network*, Protoc. Labs, 2018.
- [40] G. Wood, "Ethereum: a secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.
- [41] S. Wilkinson, J. Lowry, and T. Boshevski, *Metadisk: A Blockchain-Based Decentralized File Storage Application*, Storj Labs Inc., Technical Report, 2014.
- [42] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things," *IEEE Network Magazine*, vol. 33, no. 5, pp. 12–19, 2019.
- [43] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Consulted*, vol. 1, no. 2012, p. 28, 2008.
- [44] G. Wood, "Ethereum: a secure decentralized transaction ledger," <http://gavwood.com/paper.pdf>.
- [45] E. Ben-Sasson, A. Chiesa, C. Garman et al., "Zerocash: decentralized anonymous payments from bitcoin," in *2014 IEEE*

- Symposium on Security and Privacy*, pp. 459–474, San Jose, CA, USA, 2014.
- [46] I. Bentov and R. Kumaresan, “How to use bitcoin to design fair protocols,” in *Advances in Cryptology – CRYPTO 2014*, pp. 421–439, Springer, 2014.
- [47] R. Kumaresan and I. Bentov, “How to use bitcoin to incentivize correct computations,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, pp. 30–41, Scottsdale, AZ, USA, 2014.
- [48] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: the blockchain model of cryptography and privacy-preserving smart contracts,” in *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 839–858, San Jose, CA, USA, 2016.
- [49] R. Cleve, “Limits on the security of coin flips when half the processors are faulty,” in *Proceedings of the eighteenth annual ACM symposium on Theory of computing - STOC '86*, pp. 364–369, Berkeley, CA, USA, 1986.
- [50] G. Asharov, A. Beimel, N. Makriyannis, and E. Omri, “Complete characterization of fairness in secure two-party computation of boolean functions,” in *Theory of Cryptography*, pp. 199–228, Springer, 2015.
- [51] E. Androulaki, A. Barger, V. Bortnikov et al., “Hyperledger fabric: a distributed operating system for permissioned blockchains,” 2018, <https://arxiv.org/abs/1801.10228>.
- [52] M. Samaniego and R. Deters, “Internet of Smart Things-Iost: Using Blockchain and Clips to Make Things Autonomous,” in *2017 IEEE International Conference on Cognitive Computing (ICCC)*, pp. 9–16, Honolulu, HI, USA, 2017.
- [53] V. Buterin, “Ethereum white paper, 2013,” April 2018, <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [54] “Litecoin,” 2011, February 2018, <https://litecoin.org/>.

Research Article

An Identity-Based Anonymous Three-Party Authenticated Protocol for IoT Infrastructure

Akasha Shafiq,¹ Muhammad Faizan Ayub,¹ Khalid Mahmood ,¹ Mazhar Sadiq,¹ Saru Kumari,² and Chien-Ming Chen ³

¹Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus 57000, Pakistan

²Department of Mathematics, Chaudhary Charan Singh University, Meerut, Uttar Pradesh 250004, India

³College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

Correspondence should be addressed to Chien-Ming Chen; chienming.taiwan@gmail.com

Received 24 April 2020; Revised 18 July 2020; Accepted 29 August 2020; Published 22 September 2020

Academic Editor: Fei Yu

Copyright © 2020 Akasha Shafiq et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The rapid advancement in the field of wireless sensor and cellular networks have established a rigid foundation for the Internet of Things (IoT). IoT has become a novel standard that incorporates various physical objects by allowing them to collaborate with each other. A large number of services and applications emerging in the field of IoT that include healthcare, surveillance, industries, transportation, and security. A service provider (SP) offers several services that are accessible through smart applications from any time, anywhere, and any place via the Internet. Due to the open nature of mobile communication and the Internet, these services are extremely susceptible to various malicious attacks, e.g., unauthorized access from malicious intruders. Therefore, to overcome these susceptibilities, a robust authentication scheme is the finest solution. In this article, we introduce a lightweight identity-based remote user authentication and key agreement scheme for IoT environment that enables secure access to IoT services. Our introduced scheme utilizes lightweight elliptic curve cryptography (ECC), hash operations, and XOR operations. The theoretical analysis and formal proof are presented to demonstrate that our scheme provides resistance against several security attacks. Performance evaluation and comparison of our scheme with several related schemes for IoT environment are carried out using the PyCrypto library in Ubuntu and mobile devices. The performance analysis shows that our scheme has trivial storage and communication cost. Hence, the devised scheme is more efficient not only in terms of storage, communication, and computation overheads but also in terms of providing sufficient security against various malicious attacks.

1. Introduction

In the last few years, wireless networks have experienced tremendous growth. Nowadays, there are enormous networks associating from the cellular systems to noninfrastructure wireless systems such as sensor networks, mobile ad hoc networks, and the Internet of Things (IoT). The communication security is the key element for the success of wireless sensor applications [1, 2], especially for sensitive applications that work in mission-critical and hostile areas. Therefore, the provision of reliable and efficient security in wireless networks has always been a challenging task due to various malignant attacks and resource-constrained environment. The hasty development of wireless communication and information technologies leads to a dramatic evolution of the Internet of

Things (IoT) which is the combination of smart services and technologies that renders mutual communication among devices and users through the Internet. Since all data is shared between sensing devices and remote users via a network, therefore, it is necessary to design an efficient, secure, and lightweight remote-user authentication-based solution for an IoT environment. As far as the privacy and security of the network are concerned, mutual authentication is considered as a key element for safely accessing various IoT services. Hence, remote-user authentication becomes a vital component of various valuable services in mobile networks.

Besides confidentiality and authenticity, the exclusive features of the online valuable services raise various security questions for the remote authentication. In the environment of mobile networks where several invisible devices gather the

client's identity information, the anonymity of the client is necessarily required to make sure that the identity information of the requesting client is only known to the requested service provider (SP) and the client [3–5]. Simultaneously, when the anonymity of the client is provided, SP always wants the client's nonrepudiation for preventing the clients from the denial of charges of their desired services. The efficiency in terms of both computation and communication is crucial for such kinds of remote-user authentication schemes, especially for IoT infrastructure.

The earliest schemes employed conventional public key cryptography (PKC) [6–10]. In these schemes, clients authenticate themselves to service providers using their signature. For hiding the real identity of the clients from eavesdropping, the clients' signature and clients' identifier are encrypted using mutual secret keys between the SP and clients. The certificate of clients' public key needs to be delivered to the SP that enables the signature's verification. On the other hand, a considerable disadvantage of this approach is on-demand verification and transmission of public key certificates that cause authentication latency [11] as well as a waste of unfavorable bandwidth. In addition, to attain the clients' anonymity, encryption is required that adds to the scheme's complexity. In order to remove the drawbacks that are due to public key certificates, the modern remote-user authentication schemes employ an identity-based cryptosystem (IBC) [12–16].

IBC is another form of PKC. The IBC concept was introduced by Shamir [17] in 1984 which is swiftly evolved after Franklin and Boneh's first identity-based security-provable encryption using pairings [18]. In the IBC concept, the identity (ID) of the client serves as a client's public key, and the private key generator (PKG) generates the private key. In IBC, a pair of predefined private or public keys are generated on the basis of the user's credentials such as phone, name, or email. By using the user's unique credential or identity, the public key can be determined easily, whereas the private key generator is responsible for the generation of private keys. For communicant entities, PKG generates identity-based certificates and forwards it to the other communicants. The users involved in communication can perform encryption, generate a signature, and communicate with other users when they receive their identity-based key certificates. IBC ensures the effortless production of public and private keys. IBC removes the verification and transmission of the public key certificates; therefore, it has become a compelling substitute to conventional PKC [19]. Thus, IBC is efficient in terms of storage and transfer of certificates/public keys in comparison with the classical public key infrastructure. That is why, for a resource-constraint environment, IBC is proved to be appealing. The main advantage of IBC is there is no need of certificates. There is no need of pre-enrollment. In the traditional public key cryptography system, if the key is compromised, then the keys need to be revoked. Also, for the decryption of messages for the future, it allows postdating.

In identity-based remote-user authentication schemes, the client produces an authenticator by using his identity-based private key. The client is authorized by the SP only if verification of the client's authenticator produces an absolute

result. However, still, there are many issues that need to be resolved satisfactorily such as (i) some identity-based remote user authentication schemes consider the demand of the client's anonymity; (ii) many of those schemes introduce identity-based signature (IBS) solution and further using it as an authenticator of the client, but it remains unclear why the introduced IBS is employed rather than employing other existing IBS schemes; and (iii) no thorough quantitative argument has been given about the performance merits of such identity-based schemes over the former PKC-based schemes. Aiming to resolve the abovementioned problems, in this article, we propose an identity-based remote-user authentication scheme that targets to deliver valuable services in mobile networks. The novelty of the proposed scheme yields in its way of realizing the client's privacy without encryption operation.

1.1. Motivation. IoT serves the society with various opportunities in major fields of life, i.e., agriculture, warehousing, healthcare, and industry, that are accessible to everyone with flexibility and ease. However, this hasty development leads to the evolution of several challenges. Therefore, the fundamental motivational factors of our scheme are listed below:

- (i) IoT-based sensing devices serve with limited resources like memory, power, and battery. Therefore, an authentication scheme should have low communication and computation overheads
- (ii) Malicious attacks such as impersonation, replay, denial of services, and man-in-the-middle attacks have become enormous. Therefore, in order to resist against such attacks, the design of secure remote-user authentication scheme is the key necessity
- (iii) Furthermore, due to some components of IoT devices like actuators and sensors that deal with the crucial data of users, IoT-based applications must provide more safety and security

1.2. Our Contribution. In this article, we have proposed an identity-based anonymous three-party authenticated protocol for IoT infrastructure. The main contributions of this article are as follows:

- (1) We have presented a three-party identity-based authentication for the secure communications among users in an IoT infrastructure. The proposed identity-based scheme is designed using simple operations such as XOR, hash, and point multiplication
- (2) The proposed protocol enables mutual authentication between users and gateway for establishing and sharing the session key
- (3) User's personal credentials such as email and phone are used to generate a public key
- (4) The proposed scheme ensures the secrecy of identity such that the identity is only revealed to gateway for

authentication purpose. No adversary can get the identity

1.3. Paper Organization. The rest of the paper is organized as follows. The related work is discussed in Section 2. The preliminaries related to our paper are presented in Section 3. The generic security issues in IoT architecture are delineated in Section 4. Our introduced scheme and detailed description are given in Section 6. Section 7 presents the respective security analysis formally and informally. Thereafter, a performance comparison is highlighted in Section 8. In the end, concluding remarks are given in Section 9.

2. Related Work

The password-based authentication key exchange (PAKE) scheme [20–26] is one of the most generally known authentication key exchange (AKE) schemes, which can also be divided into three-party [27–30], two-party, and so on. In the AKE schemes, the three-party authentication key exchange (3PAKE) scheme based on password has the features of easy system maintenance, simple password, and strong expansibility. The 3PAKE scheme is extensively used in the network of modern communication. However, it is determined that the password has low entropy secret value and also prone to password guessing attack, due to the built-in issues related to the password. Therefore, due to the various problems faced by PAKE schemes, this paper reviews the identity-based schemes and introduces a three-party identity-based authentication key exchange scheme for enhancing the security.

The identity-based cryptography (IBC) [17] was developed in order to mitigate various issues associated with the conventional public key cryptography and PAKE schemes. The IBC applies the attributes of the user such as phone numbers or email addresses as public keys in order to diminish the difficulty of digital certificates, while the private key generator (PKG) creates the private keys. Therefore, the identification of user keys is critical and does not require to be revoked. Since then, the utilization of IBC remains popular for designing remote user authentication schemes. So, we review various identity-based schemes in order to find the research gap and security issues in the different infrastructures of the Internet of Things (IoT) such as edge and fog computing.

Roman et al. [31] presented the comparative summary of various security issues, challenges, and appropriate solutions for mobile edge computing (MEC) and fog computing. The readers who are interested in the details of privacy and security problems in the environment of fog computing for IoT, MEC, and mobile cloud computing (MCC) can consult [32–35], respectively. The literature emphasized the requirement of a secure mechanism for authentication. Yang and Chang [36] proposed an identity-based authentication key agreement (AKA) scheme using elliptic curve cryptosystem (ECC) for mobile devices. However, Yoon and Yoo [37] analyzed that the scheme [36] cannot resist masquerading attack and does not offer perfect forward secrecy. A pairing-free AKA scheme based on identity is introduced by Cao et al.

[38] with a minimum exchange of messages. However, Cao et al. [38] fail to offer the user untraceability and anonymity like Yang and Chang's scheme.

Tsai and Lo [39] introduced another authentication scheme based on identity for the distributed services of MCC. Their scheme uses bilinear pairing which causes high computation, but bilinear computation is performed by the server, which has usually more computing power. However, Jiang et al. [40] analyzed that a server impersonation attack cannot be resisted by their scheme [39], and also, it does not offer an appropriate mechanism of mutual authentication. Jiang et al. did not propose any improved solution, although various solutions were proposed in [41, 42].

Yang et al. [43] introduced an ECC-based scheme having the features of user untraceability and anonymity for the environment of MCC. In their scheme, a number of pseudo-IDs are assigned to a user, as well as each pseudo-ID is assigned a family of secret keys. The Access Service Network Gateway (ASN-GW) executes the predistribution process of keys. However, for each registered user, the ASN-GW requires to engender a large number of pseudo-IDs. So, the corresponding secret keys and many pseudo-IDs need to be stored by the mobile user which is impractical due to the constrained resources of mobile devices and also includes scalability issues.

Ibrahim [44] introduced an authentication scheme for the environment of fog computing, in which fog node and fog user authenticate each other. In their scheme [44], the public key infrastructure (PKI) is used to establish the secure communication channel between mobile users and registration authority, while symmetric encryption is utilized to protect the communication between fog nodes and mobile users. In their scheme, all the fog users' pregenerated secret keys are required to be stored by fog node which is also infeasible. Moreover, untraceability and anonymity are not guaranteed by their scheme. A mobile user authentication scheme is introduced by He et al. [45] for multiserver infrastructure. Their scheme uses self-certified public key cryptography which is basically identity-based cryptography. In 2017, a privacy-aware authentication scheme is introduced by Xiong et al. [46] for MCC services.

In 2019, Zhu and Geng [47] presented a three-party dynamic identity-based key exchange scheme. In 2019, Renuka et al. [48] crypt analyzed and found some attacks such as node capture, user phishing, and denial of service attacks in a three-factor authentication scheme devised by Das et al. [49] and presented an enhanced three-factor authentication scheme. Many other three-party schemes for the IoT environment have been presented [50, 51] but still lack major security features and not suitable for resource constraint environment. In 2020, Ramadan et al. [52] presented an identity-based authentication scheme for 5G systems. Kumar et al. [53] proposed an identity-based authentication scheme for cloud computing in 2020. Recently, Farjana et al. [54] presented identity-based schemes; moreover, many other schemes [55–60] are presented recently. In general, the design of efficient and secure identity-based authentication schemes is still a challenging task. In this article, we propose the identity-based lightweight

remote user authentication scheme for the IoT infrastructure in order to offer the secure and efficient communication, so that all the flaws in the discussed literature can be minimized.

3. Preliminaries

This section includes the basics of elliptic curve cryptography such as one-way hash function, collision resistance, and threat model. The common notations used throughout the research work in Table 1 are also given in this section.

3.1. Elliptic Curve Cryptography (ECC). There is a lot of public key cryptography techniques like Rivest Shamir Adleman (RSA), Diffie Hellman, and Digital Signature Algorithm (DSA). The majority of these techniques are heavy in computation. The ECC system's robustness can be anticipated based on the complexity of ECDLP (Elliptic Curve Discrete Logarithm Problem). Suppose $E_p(e, f): h^2 + eg + f \pmod p$, ECC is based on random points chosen on an elliptic curve, whereas $e, f \in Z_p$ and $4e^3 + 27f^2 \pmod p \neq 0$ for p (large prime number). The curve is defined by both the points e, f . The former equation must be verified by the points (g, h) over $E_p(e, f)$. Through repetitive addition, scalar multiplication is achieved such as $qS = S + S + S + S + S + \dots + S$ (q times), where S is a point over $E_p(e, f)$ and $q \in F_p$. The field parameters (p, e, f, S, q) belongs to the field (F_p) .

Definition 1. Discrete logarithm problem aimed at ECDLP.

Two specified random points $S, R \in E_p(e, f)$, calculate a scalar (q) such that $S = qR$. During the polynomial time (t), the benefits of $\mathcal{U}_{A_{adv}}$ is given as: $\text{Adv}_{\mathcal{U}_{A_{adv}}}^{\text{ECDLP}}(t) = \text{Prb}[(\mathcal{U}_{A_{adv}})(S, R) = x : x \in Z_p]$. The supposition of ECDLP states that $\text{Adv}_{\mathcal{U}_{A_{adv}}}^{\text{ECDLP}}(t) \leq \epsilon$.

3.2. One-Way Hash Function. Hash functions are used to get an output (f) of fixed size. Hash functions can be applied to any random argument or string (y) of any size such as $f = h(y)$. A small change in y can make a huge difference in resultant f . Subsequent parameters should be found for a secure function of hash.

- (1) If y is defined, then it is not difficult to calculate $f = h(y)$
- (2) If $f = h(y)$ is defined, then it is impossible to find out y
- (3) If $h(y_1) = h(y_2)$ is defined, then it is a tiresome task to know the specific input y_1, y_2 . The defined property is also referred to as collision resistance

Definition 2. Collision resistance characteristics aimed at hash function.

Hash function $h(\cdot)$ is secured by predefined collision resistance. The chances that an adversary ($\mathcal{U}_{A_{adv}}$) can find

TABLE 1: Common notations.

Notation	Description
\mathcal{U}_i	\mathcal{U}_i 'th remote user of the system
ID_i	\mathcal{U}_i 's identity
$\mathcal{T}\mathcal{P}\mathcal{M}_i$	\mathcal{U}_i 's tamper proof on-board memory/storage
$\mathcal{G}\mathcal{W}\mathcal{N}$	Gateway node
$ID_{\mathcal{G}\mathcal{W}\mathcal{N}}$	$\mathcal{G}\mathcal{W}\mathcal{N}$'s identity
x	$\mathcal{G}\mathcal{W}\mathcal{N}$'s secret key
$\text{Pub} = xG$	$\mathcal{G}\mathcal{W}\mathcal{N}$'s public key
$E_p(e, f)$	An elliptic curve
G	Base-point of elliptic curve $E_p(e, f)$
$h(\cdot)$	One-way function
\oplus	XoR operator
\parallel	Concatenation operator
\Rightarrow	Secure channel
\rightarrow	Public channel
$\mathcal{U}_{A_{adv}}$	Adversary

out a couple $(y_1 \neq y_2)$ as $h(y_1) = h(y_2)$ is defined as $\text{Adv}_{\mathcal{U}_{A_{adv}}}^{\text{hash}}(t) = \text{Prb}[(y_1, y_2) \leftarrow_r \mathcal{U}_{A_{adv}} : (y_1 \neq y_2) \text{ and } h(y_1) = h(y_2)]$, whereas $\mathcal{U}_{A_{adv}}$ is allowed to select a couple y_1, y_2 randomly. $\mathcal{U}_{A_{adv}}$'s advantage is determined over a random selection in polynomial time (t). Collision resistance is stated as $\text{Adv}_{\mathcal{U}_{A_{adv}}}^{\text{hash}}(t) \leq \epsilon$, whereas $\epsilon > 0$ is an adequately small value.

3.3. Identity-Based Cryptography (IBC). IBC was introduced by Shamir in 1984 [17]. It is one of the types of public key cryptography. IBC has the following properties:

- (1) Identity-based cryptosystems use user's personal credentials such as email, name, or phone number for deriving public/private keys
- (2) The public key is generated by predefined user's identity or personal credentials
- (3) Third parties or trusted authorities as PKG are responsible for the generation of private keys
- (4) PKG generates identity-based certificates, and using these certificates, encryption, generation digital signatures, and mutual authentication are performed
- (5) IBC is cost-efficient in terms of transfer and storage of keys as compared to other traditional PKI systems

3.4. Threat Model. In order to understand the capabilities of an adversary, we have used Dolev-Yao's [61] threat model. The capabilities of $\mathcal{U}_{A_{adv}}$ are as follows:

- (1) $\mathcal{U}_{A_{adv}}$ has full control over the public channel

- (2) U_{Adv} can easily intercept the messages of all the participants during communication over the public channel
- (3) U_{Adv} can be trusted or deceitful user of the system
- (4) U_{Adv} can be an insider of the system
- (5) The identities are publicly known
- (6) U_{Adv} cannot find or extract x (GWN's private key)
- (7) U_{Adv} cannot access the messages that are being transmitted over a secure channel

4. Security Issues in IoT

In the design of IoT applications, IoT's security is the most important thing. Therefore, the major challenge which requires serious consideration is to provide strong security for IoT. In the Internet world, IoT has a very bright future. Thus, for the realization of services of modern technologies and their benefits, security requirements such as authentication and privacy are much important.

Therefore, subsequent issues must be handled with consideration.

4.1. Common Vulnerabilities in IoT Architecture. The devices of IoT existing in an abandoned environment require active inspection of every feasible condition in which the attacker can attack on devices of IoT. As per detailed scrutiny, we can wrap up the vulnerabilities of IoT as follows:

- (i) *Impersonation Attack.* A malignant hacker can masquerade as a service provider or a user by responding to an authentic request from old transmission between any two legal entities. Therefore, a malignant hacker can enjoy the same services as a legitimate user or service provider.
- (ii) *Denial of Service Attack.* The attacker by flooding the network with previous login requests or information exchanged between two entities can reduce the network's performance and can make the services unavailable.
- (iii) *Eavesdropping Attack.* The attacker can listen to private communication on a public channel and can misuse it later to attack a user or server.
- (iv) *Man-in-Middle Attack (MITM).* The adversary can forge the message exchanged between the gateway and user, later using this information can impersonate as a legal gateway/server and user using different techniques.
- (v) *Parallel Session Attack.* An attacker can eavesdrop the messages between the system of IoT and then attempts to generate a session to get the old data.
- (vi) *Gateway Node Bypassing Attack.* To obtain IoT sensitive information and services without authentication

of a gateway, an attacker can try to access the system by bypassing the gateway.

- (vii) *Stolen Smart Device Attack.* An attacker can derive the user's personal data from smart devices and utilize it later to impersonate as a legitimate user of the network.
- (viii) *Offline Guessing Attack.* Using an offline dictionary attack, the adversary can attempt to get access to the system of IoT by guessing all possible passwords.

4.2. Security Feature Requirements in IoT. Many security features must be incorporated while designing the authentication schemes. The following is a list of important security features that can be exploited to design an efficient and secure scheme.

- (i) *User Anonymity.* The participant's identity must be secured such that if an attacker tries to eavesdrop the message and intercept message during the login and authentication stage. If the identity is revealed, then the attacker can misuse it and the user's privacy is breached.
- (ii) *Mutual Authentication.* Two participating entities must mutually authenticate each other to avoid security threats.
- (iii) *Availability.* Whenever a user requires to access the system, all IoT resources should be available.
- (iv) *Confidentiality.* The user's personal and sensitive information must be protected and should be visible only to legitimate users.
- (v) *Scalability.* The system of authentication must be responsive to the modification occurring in the network, and the system should be allowed to grow dynamically according to the modifications that are being happened.
- (vi) *Forward Secrecy.* The access to entities in any authentication scheme is granted by sharing the session key. That is why the old session keys cannot be used to initiate a new session.
- (vii) *Resistance to Attacks.* A secure authentication scheme must resist the major security threats such as the Distributed Denial of Services (DDoS), MITM, impersonation, and stolen verifier attack.

5. System Setup

In an IoT infrastructure, gateway plays an important role to ensure the security in the network. Our presented model consists of two participants as shown in Figure 1, such as IoT nodes and gateway. In general, IoT nodes have limited resources in terms of computation, communication, and power. The IoT nodes aimed to communicate with each other by authenticating via a trusted gateway. As in Figure 1, IoT node (1) and IoT node (a) initiate a session

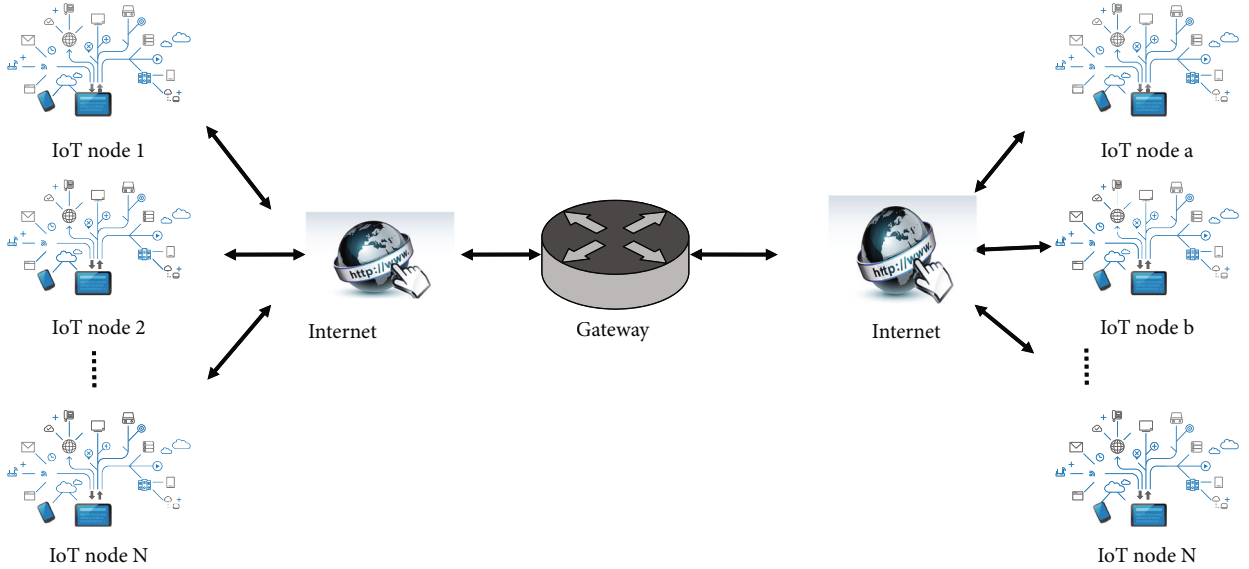


FIGURE 1: System setup for the proposed scheme.

by sending a login request to the gateway. The gateway is responsible for establishing a secure communication between IoT nodes. Once the IoT nodes are authenticated by the gateway, the IoT nodes can then securely communicate with each other. Due to the public nature and limited resources, the IoT nodes face several security and privacy challenges. The generic three-party IoT infrastructure for remote-user authentication is demonstrated in Figure 1. Suppose a remote user wants to communicate with another remote user, then they both have to pass the authentication process. For this purpose of authentication, each entity will be verified through gateway node GWN. If both entities have been authenticated, then the GWN sends a challenge message to both entities. Upon receiving the challenge message, each entity authenticates the GWN and computes a session key. In the end, both users agreed on this common shared session key.

6. The Proposed Scheme

In this section, we elaborated on our proposed identity-based scheme which upholds user anonymity, user untraceability, perfect forward secrecy, key agreement, and mutual authentication. The introduced scheme comprises of these phases: Section 6.1 the registration phase and Section 6.2 the login and authentication phase. These two phases are described below in detail.

6.1. Registration Phase. If a user \mathcal{U}_a wants to communicate with another user \mathcal{U}_b , then they both have to pass the authentication process. For authentication, each entity will be verified by \mathcal{GWN} . If both entities are authenticated, then they can share the session key. The complete registration process of the user \mathcal{U}_i of the proposed scheme is described in detail in this subsection. Figure 2 shows the registration phase of the proposed scheme. The registration process consists of the following steps:

RG-Step 1. \mathcal{U}_i chooses his/her ID_i and the arbitrary number l_{i1} .

RG-Step 2. \mathcal{GWN} upon receiving the registration requests $(ID_i, h(ID_i \oplus l_{i1}))$ from U_i , then calculates the following values:

$$\begin{aligned} MID_i &= h(ID_i), \\ V_i &= h(x \| MID_i), \\ Y_i &= V_i \oplus h(ID \oplus l_{i1}) \end{aligned} \quad (1)$$

RG-Step 3. On receiving Y_i from GWN, U_i calculates the following values:

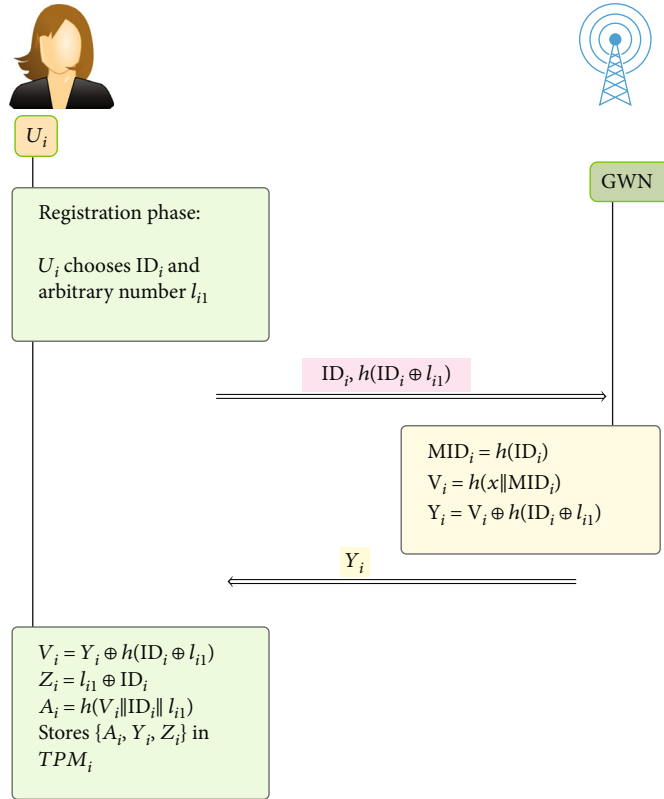
$$\begin{aligned} V_i &= Y_i \oplus h(ID_i \oplus l_{i1}), \\ Z_i &= l_{i1} \oplus ID_i, \\ A_i &= h(V_i \| ID_i \| l_{i1}) \end{aligned} \quad (2)$$

After calculating these values, stores $\{A_i, Y_i, Z_i\}$ in \mathcal{TPM}_i .

6.2. Login and Authentication Phase. The complete process of login and authentication of the introduced scheme as presented in Figure 3 is elaborated in this subsection which consists of the following steps:

AT-Step 1. Both U_a and U_b input their identity (ID_a, ID_b) , respectively. Then, U_a calculates the following values on the basis of the credentials stored in tamper proof on-board memory \mathcal{TPM}_i of the mobile device [62, 63]:

$$\begin{aligned} l_{a1} &= Z_a \oplus ID_a, \\ V_a &= Y_a \oplus h(ID_a \oplus l_{a1}), \\ A_a &\stackrel{?}{=} h(V_a \| ID_a \| l_{a1}) \end{aligned} \quad (3)$$

FIGURE 2: Registration process of U_i .

Further computation generates a random number l_{a2} and calculates the following values:

$$\begin{aligned} Q_a &= l_{a2}G, \\ PID_a &= (ID_a || MID_b) \oplus l_{a2}Pub, \\ auth_a &= h(ID_a || MID_b || ID_{GWN} || V_a) \end{aligned} \quad (4)$$

whereas U_b calculates the following values on the basis of the credentials entered during the registration process.

$$\begin{aligned} l_{b1} &= Z_b \oplus ID_b, \\ V_b &= Y_b \oplus h(ID_b \oplus l_{b1}), \\ A_b &\stackrel{?}{=} h(V_b || ID_b || l_b) \end{aligned} \quad (5)$$

Further, U_b generates a random number l_{b2} and computes the following values:

$$\begin{aligned} Q_b &= l_{b2}G, \\ PID_b &= (ID_b || MID_a) \oplus l_{b2}Pub, \\ auth_b &= h(ID_b || MID_a || ID_{GWN} || Y_b \oplus h(ID_b || l_{b1})) \end{aligned} \quad (6)$$

After calculating these values, \mathcal{U}_a and \mathcal{U}_b send login request $\{auth_a, Q_a, PID_a\}$ and $\{auth_b, Q_b, PID_b\}$, respectively, towards the gateway.

AT-Step 2. After receiving login requests from U_a , the GWN calculates the following values for U_a :

$$\begin{aligned} xQ_a &= l_{a2}xG = l_{a2}Pub, \\ (ID_a || MID_b) &= PID_a \oplus l_{a2}Pub, \\ MID_a &= h(ID_a), \\ auth_a &\stackrel{?}{=} h(ID_a || MID_b || ID_{GWN} || h(x || MID_a)) \end{aligned} \quad (7)$$

Also, calculate the following values for \mathcal{U}_b upon receiving the login request $\{auth_b, Q_b, PID_b\}$

$$\begin{aligned} xQ_b &= l_{b2}xG = l_{b2}Pub, \\ (ID_b || MID_a) &= PID_b \oplus l_{b2}Pub, \\ MID_b &= h(ID_b), \\ auth_b &\stackrel{?}{=} h(ID_b || MID_a || ID_{GWN} || h(x || MID_b)) \end{aligned} \quad (8)$$

Further, the \mathcal{GWN} generates l_{GWN} and calculate the following values as:

FIGURE 3: Login and authentication process of U_i .

$$\begin{aligned}
M_{GWN} &= (ID_{GWN} \| x \| l_{GWN}), \\
N_{GWN1} &= M_{GWN} \oplus V_a, \\
N_{GWN2} &= M_{GWN} \oplus V_b, \\
\text{auth}_{GWN1} &= h(ID_a \| ID_{GWN} \| V_a \| M_{GWN}), \\
\text{auth}_{GWN2} &= h(ID_b \| ID_{GWN} \| V_b \| M_{GWN})
\end{aligned} \tag{9}$$

AT-Step 3. After the calculation of the above values, \mathcal{EWN} sends $\{\text{auth}_{GWN1}, Q_b, N_{GWN1}\}$ and $\{\text{auth}_{GWN2}, Q_a, N_{GWN2}\}$ to \mathcal{U}_a and \mathcal{U}_b , respectively. \mathcal{U}_a then calculates the following values along with the session key:

$$\begin{aligned}
M_{GWN} &= N_{GWN2} \oplus V_a, \\
\text{auth}_{GWN1} &\stackrel{?}{=} h(ID_a \| ID_{GWN} \| V_a \| M_{GWN}), \\
k &= l_{a2} Q_b, \\
SK_{ab} &= h(MID_a \| MID_b \| ID_{GWN} \| k)
\end{aligned} \tag{10}$$

Also, \mathcal{U}_b on the basis of the received parameters $\{\text{auth}_{GWN2}, Q_a, N_{GWN2}\}$ calculates the following values along with the session key:

$$\begin{aligned}
M_{GWN} &= N_{GWN2} \oplus V_b, \\
\text{auth}_{GWN2} &\stackrel{?}{=} h(ID_b \| ID_{GWN} \| V_b \| M_{GWN}), \\
k &= l_{b2} Q_a, \\
SK_{ab} &= h(MID_a \| MID_b \| ID_{GWN} \| k),
\end{aligned} \tag{11}$$

Finally, \mathcal{EWN} computes a shared session key as:

$$SK_{ab} = h(MID_a \| MID_b \| ID_{GWN} \| k) \tag{12}$$

Hence, both the entities \mathcal{U}_a and \mathcal{U}_b authenticate themselves via \mathcal{EWN} and consequently shared a session key for subsequent communication.

7. Security Analysis

This section presents the formal and informal security analysis of the proposed scheme. We have used Real-Or-Random (ROR) [64] in order to prove the security of the proposed scheme. Furthermore, informal security analysis shows that the proposed scheme provides resilience against all known attacks.

7.1. Informal Security Analysis. The security of the proposed scheme is analyzed informally in this section. The informal security analysis represents the proposed scheme's correctness and ensures that it resists various attacks.

7.1.1. Identity Security. The abundance of resource-constrained devices among the advanced communication infrastructures has made the existing protocol incompatible for diverse real-time applications like IoT and smart grid. Therefore, the demand for lightweight solutions is on the peak, IBC is one of them. It is a new way to solve these prob-

lems without any complex computation. That is why it has grabbed the attention of the researchers. For achieving confidentiality, the personal information for identification should be sent via a secure channel. The respective U_i has the private key corresponding to his/her own ID_i . Also, identity security includes the availability of identity. If a U_i 's identity is revoked by GWN, even then, the U_i has control over his ID_i and the relevant claims, which states that the U_i still can use his/her ID_i in other applications.

7.1.2. Key Agreement. After completing the successful process of mutual authentication, a common session key SK is shared between the users. This shared session key is established through $SK_{ab} = h(MID_a k MID_b k ID_{GWN} k k)$. Hence, our scheme offers a successful key agreement.

7.1.3. Mutual Authentication. In our introduced scheme, the \mathcal{EWN} can authenticate \mathcal{U}_a by verifying $\text{auth}_a = ? h(ID_a \| MID_b \| ID_{GWN} \| V_a)$. The values $ID_a, MID_b, ID_{GWN}, V_a$ are only known to valid \mathcal{U}_a , as an adversary cannot calculate all these values. So, only legitimate user \mathcal{U}_a can be authenticated by \mathcal{EWN} . Likewise, \mathcal{EWN} authenticates the other user. Similarly, user \mathcal{U}_a can also authenticate \mathcal{EWN} by verifying $\text{auth}_{GWN} = ? h(ID_a \| ID_{GWN} \| V_a \| M_{GWN})$. The values $ID_a, ID_{GWN}, V_a, M_{GWN}$ are only known to valid \mathcal{U}_a . As adversary cannot calculate all these values, so only the legitimate \mathcal{EWN} can be authenticated by \mathcal{U}_a . Likewise, other users can authenticate \mathcal{EWN} . Thus, it is proved that our introduced scheme offers mutual authentication between users and \mathcal{EWN} .

7.1.4. User Anonymity. During the login and authentication stage, the identity of \mathcal{FID}_a of user \mathcal{U}_a is not transmitted in plain text; instead, the pseudonymity PID_a is sent over the public channel. Furthermore, the identity of \mathcal{U}_a is not stored in temper proof onboard memory/storage. That is why adversary cannot retrieve the identity of \mathcal{U}_a without having the private key. So, our proposed scheme provide user anonymity.

7.1.5. User Untraceability. During the design of the authentication scheme, untraceability is considered as an important factor. The proposed scheme provides user's untraceability because in each login session \mathcal{U}_a computes unique PID_a , it is clear that \mathcal{U}_a does not transmit the same dynamic identity instead every time session-specific random number is used to calculate PID_a . So, it cannot be guessed by any adversary that two different sessions are established by the same or different users.

7.1.6. Perfect Forward Secrecy. In our introduced scheme, if $\mathcal{U}_{A_{adv}}$ is able to know the secret parameters such as the secret key of \mathcal{EWN} , even then, he cannot determine the former session keys. In the proposed scheme, arbitrary numbers $\{l_{a1}, l_{a2}\}$ are used to compute the valid value of k that is further used in the computation of SK_{ab} . Due to the usage of random numbers, different session keys are generated in each session. So, even after getting the secret parameter, the adversary cannot guess the previous session keys.

7.1.7. Backward Secrecy. In the introduced scheme, if $\mathcal{U}_{A_{adv}}$ is able to find the secret parameters of \mathcal{GWN} , even then, he cannot find the future sessions. In the proposed scheme, the calculation of valid Sk_{ab} requires arbitrary number $\{l_{a1}, l_{a2}\}$. Due to these random numbers, the session key is specific for every session; thus, $\mathcal{U}_{A_{adv}}$ cannot find future session keys.

7.1.8. Privileged Insider and Stolen Verifier Attack. During the registration phase, \mathcal{U}_i transmit ID_i and l_{i1} through the private channel to \mathcal{GWN} , where arbitrary number l_{i1} is generated by \mathcal{U}_i . Furthermore, for \mathcal{U}_i 's identity, no table is preserved, for authentication \mathcal{GWN} uses x his secret key. Thus, no insider $\mathcal{U}_{A_{adv}}$ can get access to the user's identity and credentials. Hence, the introduced scheme resists stolen verifiers and privileged insider attacks.

7.1.9. User Masquerading Attack. Suppose $\mathcal{U}_{A_{adv}}$ tries to masquerade a legal \mathcal{U}_a by means of sending a legal login request message on behalf of \mathcal{U}_a to the \mathcal{GWN} . In order to produce an original login message $\{auth_a, Q_a, PID_a\}$, the adversary needs to calculate valid $auth_a = h(ID_a \| MID_b \| ID_{GWN} \| V_a)$. It is not possible for the adversary to calculate $auth_a$ because $\mathcal{U}_{A_{adv}}$ does not know ID_a of \mathcal{U}_a . Likewise, the other user is also secured from impersonating by an adversary. So, the proposed scheme has the ability to withstand the user masquerading attack.

7.1.10. \mathcal{GWN} Masquerading Attack. Suppose an attacker $\mathcal{U}_{A_{adv}}$ tries to impersonate a legal server \mathcal{GWN} by means of sending a legal challenge message on the behalf of \mathcal{GWN} to the user. In order to produce an original challenge message $\{auth_{GWN}, Q_a, N_{GWN}\}$, the adversary needs to calculate the valid $auth_{GWN} = h(ID_a \| ID_{GWN} \| V_a \| M_{GWN})$. However, this operation is computationally expensive because for determining $V_a = h(x \| MID_a)$, it needs a private key of \mathcal{GWN} . So, the proposed scheme has the ability to withstand the user masquerading attack.

7.1.11. Man-in-the-Middle Attack (MITM). Suppose $\mathcal{U}_{A_{adv}}$ forges the login message $\{auth_a, Q_a, PID_a\}$ sent by \mathcal{U}_a to \mathcal{GWN} , still, any tampering in the login request message will easily be identified while determining $auth_a = h(ID_a \| MID_b \| ID_{GWN} \| V_a)$. $\mathcal{U}_{A_{adv}}$ requires the user's identity which is unknown to adversary. Likewise, the other user is also secure against this attack. So, the proposed scheme is secured against MITM.

7.1.12. Replay Attack. If $\mathcal{U}_{A_{adv}}$ intercepts the request message $\{auth_a, Q_a, PID_a\}$ of \mathcal{U}_i and later replays the intercept message, the calculation of Q_a and PID_a includes a random number l_a which is session specific. Because of the random number, the values of the entities will always be different for every session. Hence, a replay attack is not possible on the proposed scheme.

7.1.13. Parallel Session Attack. Suppose the scheme's parallel session is tried to be constructed by $\mathcal{U}_{A_{adv}}$, but this scenario is not possible in the proposed scheme as a unique identity is utilized. Therefore, even one valid session cannot be run by

$\mathcal{U}_{A_{adv}}$ to masquerade a legitimate user. Thus, a parallel session attack can be efficiently resisted by the proposed scheme.

7.1.14. No Clock Synchronization. In the proposed scheme, session-specific random numbers are used in every session instead of a time stamp. So, no clock synchronization is required.

7.2. Formal Security Analysis. In this subsection, we prove that our scheme is AKA-Secure if the ECDHP is a hard problem. We present this proof under the (BRP) [64, 65] and Abdalla et al.'s [66] security model.

Theorem 2. Let the proposed scheme be denoted as \mathcal{P}_p . If $\mathcal{U}_{A_{adv}}$ is an attacker who builds at most q_{send} Send queries, q_{rvt} Reveal queries, q_{exe} Execute queries, q_{hash} Hash queries and succeed the game having benefit $Adv_{\mathcal{P}_p}^{AKA}(\mathcal{U}_{A_{adv}})$, then an algorithm that should be existed, which can efficiently resolve ECDHP hard problem on group G having benefit Adv_G^{ECDHP} , where

$$Adv_{\mathcal{P}_p}^{AKA} \leq \frac{q_{hash}^2}{2^l - 1} + \frac{q_{send}}{2^{l-2}} + \frac{(q_{send} + q_{exe})^2}{P} + \frac{(q_{send} + q_{exe})^2}{P} + 2q_{hash} Adv_G^{ECDHP} \quad (13)$$

Proof. Suppose, for the base point G and elliptic group E_p there exists an ECDHP instance (P, aP, bP) , we make a challenge \mathcal{C}_r who wishes to calculate abP using $\mathcal{U}_{A_{adv}}$ as a function. The function that is taken as an arbitrary oracle in the proposed scheme is referred to as hash $h(\cdot)$. In order to record the hash queries and their answer, \mathcal{C}_r maintains a hash list and is referred to as a L_{hash} . To make it simple, we use three transcripts between entities, which are as follows:

$$m\mathcal{U}_a = \{auth_a, Q_a, PID_a\},$$

$$m\mathcal{U}_b = \{auth_b, Q_b, PID_b\},$$

$$m\mathcal{GWN} = \{auth_{GWN_1}, Q_b, N_{GWN_1}, auth_{GWN_2}, Q_a, N_{GWN_2}\} \quad (14)$$

After simulating the scheme, \mathcal{C}_{rs} answers the queries questioned by $\mathcal{U}_{A_{adv}}$ as follows:

(i) *Hash Query.* after getting the hash query with input m from $\mathcal{U}_{A_{adv}}$, \mathcal{C}_r scans the L_{Hash} . \mathcal{C}_r returns r to $\mathcal{U}_{A_{adv}}$ if entry $(m, r) \in L_{Hash}$; otherwise, \mathcal{C}_r selects r randomly and gives r back to $\mathcal{U}_{A_{adv}}$ and adds (m, r) in to L_{Hash}

(ii) *Send Query.*

(1) \mathcal{C}_r simulates $\mathcal{U}_{A_{adv}}$'s response in the following way after getting $Send(\mathcal{U}_{A_{adv}}, Start)$: selects a random numbers l_{a1}, l_{a2} and computes $Q_a = l_{a2}G$, $PID_a = (ID_a \| MID_b) \oplus l_{a2, pub}$, $auth_a = h(ID_a \| MID_b \| ID_{GWN} \| V_a)$ and returns back $\{auth_a, Q_a, PID_a\}$ as response

- (2) Upon the reception of query $\text{Send}(\mathcal{U}_b, (\text{auth}_a, Q_a, \text{PID}_a))$, assume that \mathcal{U}_b is in accurate state. \mathcal{U}_b 's response is simulated by \mathcal{E}_r as follows: selects random numbers l_{b1}, l_{b2} and computes $Q_b = l_{b2}G$, $\text{PID}_b = (\text{ID}_b \parallel \text{MID}_a) \oplus l_{b2}\text{pub}$, $\text{auth}_b = h(\text{ID}_b \parallel \text{MID}_b \parallel \text{ID}_{\text{GWN}} \parallel V_b)$ and returns back $\{\text{auth}_b, Q_b, \text{PID}_b\}$ as response
- (3) Upon getting $\text{Send}(\text{GWN}(\text{auth}_a, Q_a, \text{PID}_a))$, suppose that $\mathcal{E}\mathcal{W}\mathcal{N}$ is in true state, then the response of Send query is simulated by \mathcal{E}_r as follows: computes $xQ_a = l_{a2}xG = l_{a2}\text{pub}$, $(\text{ID}_a \parallel \text{MID}_b) = \text{PID}_a \oplus l_{a2}\text{pub}$, $\text{MID}_a = h(\text{ID}_a)$, and $\text{auth}_a = h(\text{ID}_a \parallel \text{MID}_b \parallel \text{ID}_{\text{GWN}} \parallel h(x \parallel \text{MID}_a))$. Furthermore, GWN generates l_{GWN} and computes $N_{\text{GWN}_1} = M_{\text{GWN}} \oplus V_a$, $\text{auth}_{\text{GWN}_1} = h(\text{ID}_a \parallel \text{ID}_{\text{GWN}} \parallel V_a \parallel M_{\text{GWN}})$ and response back with $\{\text{auth}_{\text{GWN}_1}, Q_b, N_{\text{GWN}_1}\}$.
- (4) After receiving query $\text{Send}(\text{GWN}, (\text{auth}_b, Q_b, \text{PID}_b))$ and assuming $\mathcal{E}\mathcal{W}\mathcal{N}$ as a correct state, \mathcal{E}_r simulates $\mathcal{E}\mathcal{W}\mathcal{N}$'s response as follows: computes $xQ_b = l_{b2}xG = l_{b2}\text{pub}$, $(\text{ID}_b \parallel \text{MID}_a) = \text{PID}_b \oplus l_{b2}\text{pub}$, $\text{MID}_b = h(\text{ID}_b)$ and verifies $\text{auth}_b = h(\text{ID}_b \parallel \text{MID}_a \parallel \text{ID}_{\text{GWN}} \parallel h(x \parallel \text{MID}_b))$. Furthermore, generate l_{GWN} and compute $N_{\text{GWN}_2} = M_{\text{GWN}} \oplus V_b$, $\text{auth}_{\text{GWN}_2} = h(\text{ID}_b \parallel \text{ID}_{\text{GWN}} \parallel V_b \parallel M_{\text{GWN}})$, and return $\{\text{auth}_{\text{GWN}_2}, Q_a, N_{\text{GWN}_2}\}$ as response
- (5) In the end, the session key is shared among the participants if checks $\text{auth}_{\text{GWN}_1} = ? h(\text{ID}_a \parallel \text{ID}_{\text{GWN}} \parallel V_a \parallel M_{\text{GWN}})$ and $\text{auth}_{\text{GWN}_2} = ? h(\text{ID}_b \parallel \text{ID}_{\text{GWN}} \parallel V_b \parallel M_{\text{GWN}})$ are hold true. Otherwise, the session will be terminated

(iii) *Execute Query.* While getting execute query (U_a, GWN, U_b) , C_r simulates the send query as follows:

$$\begin{aligned} m_{\mathcal{U}_a, g} &= \text{Send}(\mathcal{U}_a, \text{Start}), \\ m_{\mathcal{U}_b, g} &= \text{Send}(\mathcal{U}_b, m_{\mathcal{U}_a}), \\ m_g \mathcal{U}_a \mathcal{U}_b &= \text{Send}(\mathcal{E}\mathcal{W}\mathcal{N}, m_{\mathcal{U}_a, g}, m_{\mathcal{U}_b, g}) \end{aligned} \quad (15)$$

C_r returns $m_{\mathcal{U}_a, g}$, $m_{\mathcal{U}_b, g}$ and $m_g \mathcal{U}_a \mathcal{U}_b$ as an answer.

(iv) *Corrupt Query.*

- (1) On getting a query $\text{Corrupt}(\mathcal{U}_i, \{\text{ID}_i\})$, C_r responds $V_i = h(x \parallel \text{MID}_i)$
- (2) On receiving query $\text{Corrupt}(\text{GWN}, \{V_i\})$, C_r responds all information stored in temper proof onboard storage/memory

(v) *Reveal query:* after getting a query $\text{Reveal}(U_i)$, C_r responds SK_{ab} if the instance is accepted; otherwise, \perp will be responded.

TABLE 2: Desktop device specifications.

Item	Specification
Processor	i7 3.60 GHz
RAM	8 GB
Operating system	Ubuntu

TABLE 3: Mobile device specifications.

Item	Specification
Mobile device	Vivo S1
Processor	Octa-Core
ROM	128 GB
RAM	6 GB

(vi) *Test query:* upon the reception of query $\text{Test}(U_i)$, toss up a coin $b \in \{0, 1\}$. The right session key SK_{ab} will be returned if $b = 1$. Otherwise, an arbitrary value of the same size will be returned.

A game sequence $G_{a0}, G_{a1}, \dots, G_{a5}$ is defined next. For every game G_{ai} , assume S_i is an event that U_{Adv} wins the game, which means U_{Adv} predicted b successfully. The following is the description:

Game G_{a0} . This game is the original attack game constructed by (BRP) [64, 65] and Abdalla et al.'s [66] security model, where the hash functions are modeled as a random oracle. According to the definition, we got:

$$\text{Adv}_{\mathcal{U}_{\text{Adv}}} = |2P_r[S_0] - 1| \quad (16)$$

Game G_{a1} . G_{a1} is similar to G_{a0} , but the difference is that hash queries are entertained by scanning the L_{hash} by C_r . G_{a1} remains indistinguishable from G_{a0} until the queries are answered similarly in G_{a0} . Hence, we got

$$P_r[S_1] = P_r[S_0] \quad (17)$$

Game G_{a2} . G_{a2} is similar to G_{a1} . But, the difference is that G_{a2} 's simulation terminates if subsequent events occur:

- (i) *Event_1.* Collision of hash queries during simulation.
- (ii) *Event_2.* Collision on the simulation of transcripts $m_{\mathcal{U}_a, g}, m_{\mathcal{U}_b, g}, m_g \mathcal{U}_a \mathcal{U}_b$.

As per the concept of birthday paradox, we got $P_r[\text{Event}_1] \leq q_{\text{hash}}^2 / 2^{l+1}$. For transcript $m_g \mathcal{U}_a \mathcal{U}_b$, the collision probability of Event_2 is $(q_{\text{send}} + q_{\text{exe}})^2 / 2^{p^2}$, while the probability

TABLE 4: Computation Cost of Proposed and Related Schemes.

Schemes	No. of operations at U_i	No. of operation at GWN	Total no. of operations	Total time (ms)
Ours	$5h(\cdot) + 3PM$	$4h(\cdot) + 2PM$	$9h(\cdot) + 5PM$	44.0094
He et al. [67]	$6h(\cdot) + 4PM$	$8h(\cdot) + 8PM$	$14h(\cdot) + 12PM$	56.0296
Challa et al. [68]	$8h(\cdot) + 5PM$	$4h(\cdot) + 4PM$	$12h(\cdot) + 9PM$	72.0148
Ma et al. [69]	$4h(\cdot) + 3PM$	$9h(\cdot) + 6PM$	$13h(\cdot) + 9PM$	40.0253
Taher et al. [70]	$9h(\cdot)$	$6h(\cdot)$	$15h(\cdot)$	36.0062
Chandrakar and Om [71]	$11h(\cdot) + 4PM$	$6h(\cdot) + 4PM$	$17h(\cdot) + 8PM$	76.0169
Lu et al. [72]	$8h(\cdot) + 4PM$	$6h(\cdot) + 1PM$	$14h(\cdot) + 5PM$	64.0088
Mo and Chen [73]	$13h(\cdot) + 1PM$	$10h(\cdot)$	$23h(\cdot) + 1PM$	60.0103

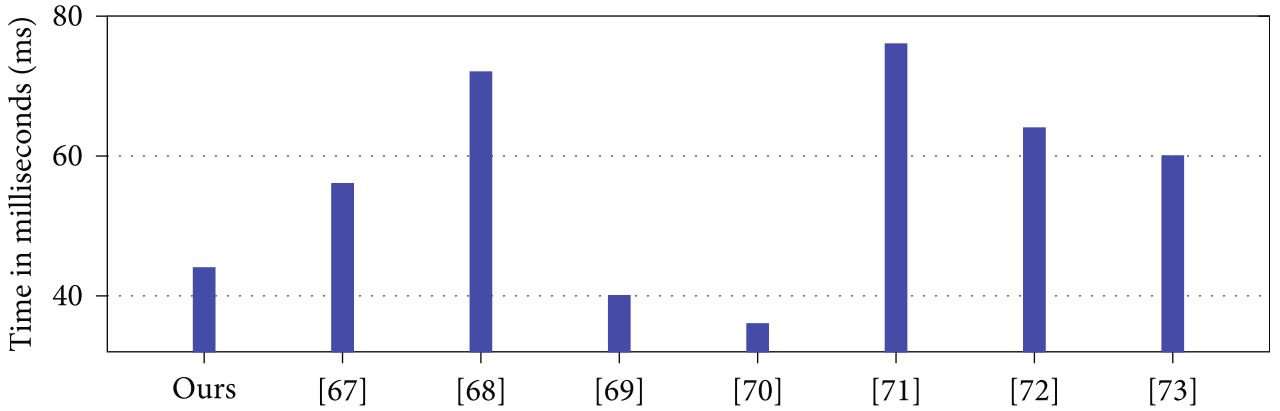


FIGURE 4: Comparison of the proposed and related scheme computation overhead.

TABLE 5: Communication structure.

Schemes	Communication structure
Ours	$U_i \rightarrow \mathcal{EWN} \rightarrow U_i$
He et al. [67]	$U_i \rightarrow S_j \rightarrow \mathcal{EWN} \rightarrow S_j \rightarrow U_i$
Challa et al. [68]	$U_i \rightarrow TA \rightarrow S_j$
Ma et al. [69]	$U_i \rightarrow S_j \rightarrow CS \rightarrow S_j \rightarrow U_i$
Taher et al. [70]	$U_i, S_j \rightarrow \mathcal{EWN} \rightarrow U_i, S_j$
Chandrakar and Om [71]	$U_i \rightarrow \mathcal{EWN} \rightarrow S_j \rightarrow \mathcal{EWN} \rightarrow U_i$
Lu et al. [72]	$U_i \rightarrow \mathcal{EWN} \rightarrow S_j \rightarrow U_i$
Mo and Chen [73]	$U_i \rightarrow \mathcal{EWN} \rightarrow S_j \rightarrow \mathcal{EWN} \rightarrow U_i$

of collision on the transcript $m_{\mathcal{U}_a}, m_{\mathcal{U}_b}$ is $(q_{\text{send}} + q_{\text{exe}})^2 / 2p$. We got:

$$|P_r[S_2] - P_r[S_1]| \leq \frac{q_{\text{hash}}^2}{2^{l+1}} + \frac{(q_{\text{send}} + q_{\text{exe}})^2}{2p^2} + \frac{(q_{\text{send}} + q_{\text{exe}})^2}{2p} \quad (18)$$

Game G_{a3} . G_{a3} is almost similar to G_{a2} , but the difference is that, $\mathcal{U}_{A_{\text{adv}}}$ may know the authentication value auth_a , aut

h_b , $\text{auth}_{\text{GWN}_1}$ and $\text{auth}_{\text{GWN}_2}$ without knowing the hash oracle. Thus, we got

$$|P_r[S_3] - P_r[S_2]| \leq \frac{q_{\text{send}}}{2^l} \quad (19)$$

Game G_{a4} . In G_{a4} , G_{a3} is modified as follows:

- (i) \mathcal{U}_a scans L_{Hash} for ID_a . If the entries exist, then calculate $\{\text{auth}_a, Q_a, \text{PID}_a\}$
- (ii) GWN verifies the legitimacy of \mathcal{U}_a . If it holds, then GWN scans for $\{\text{auth}_a, Q_a, \text{PID}_a\}$ in the Send list. Otherwise, the session aborts. G_{a4} will succeed if $\mathcal{U}_{A_{\text{adv}}}$ guess the authentication parameters without a hash oracle. So

$$|P_r[S_4] - P_r[S_3]| \leq \frac{q_{\text{send}}}{2^l} \quad (20)$$

GAME G_{a5} . In G_{a5} , the G_{a4} is modified as follows:

- (i) \mathcal{U}_a randomly chooses l_{a2} and computes $Q_a = l_{a2}G$, $\text{PID}_a = (\text{ID}_a \parallel \text{MID}_a) \oplus l_{a2}\text{pub}$, and $\text{auth}_a = h(\text{ID}_a \parallel \text{MID}_a \parallel \text{ID}_{\text{GWN}} \parallel Y_a \oplus h(\text{ID}_a \parallel l_{a1}))$ and stores $\{\text{auth}_a, Q_a, \text{PID}_a\}$ in L_{Hash}

TABLE 6: Communication cost of the proposed and related schemes.

Schemes	No. of messages exchanged	Cost of registration phase	Cost of login authentication	Total cost
Ours	3	672	1344	2016
He et al. [67]	6	928	3776	4704
Challa et al. [68]	5	512	2976	3488
Ma et al. [69]	8	832	4704	5536
Taher et al. [70]	8	3392	5440	8832
Chandrakar and Om [71]	8	2368	3360	5728
Lu et al. [72]	5	672	2944	3616
Mo and Chen [73]	6	2112	4504	6616

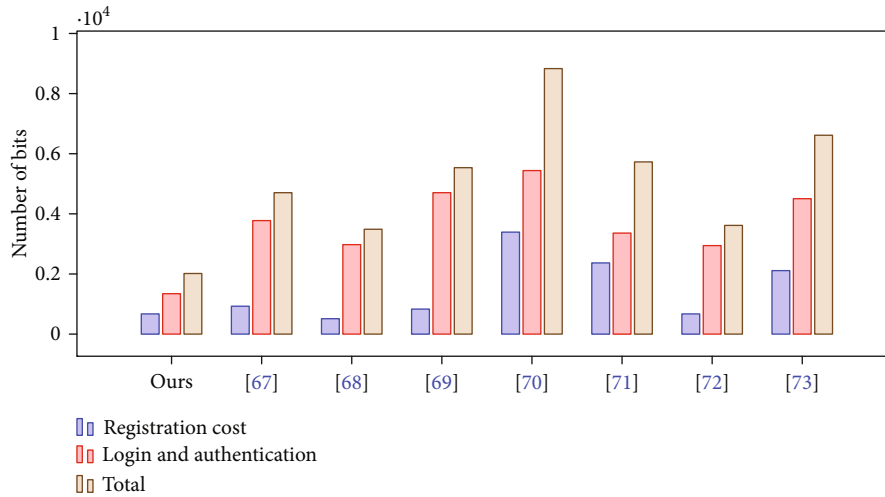


FIGURE 5: Comparison of proposed and related scheme communication overhead.

TABLE 7: Storage cost of the proposed and related schemes.

Schemes	No. of bits required for storage
Ours	672
He et al. [67]	672
Challa et al. [68]	1024
Ma et al. [69]	672
Taher et al. [70]	1536
Chandrakar and Om [71]	1856
Lu et al. [72]	768
Mo and Chen [73]	2464

- (ii) \mathcal{U}_b randomly selects l_{b2} and computes $Q_{b2} = l_{b2}G$, $PID_b = (ID_b \| MID_a) \oplus l_{b2}pub$, and $auth_b = h(ID_b \| MID_a \| ID_{GWN} \| Y_b \oplus h(ID_b \| l_{b1}))$ and stores $\{auth_b, Q_b, PID_b\}$ in L_{Hash}

Now, the updated G_{a5} is indistinguishable from G_{a4} until $\mathcal{U}_{A_{adv}}$ asks a hash oracle on abP , whose probability is $1/q_{hash}$. So

$$|P_r[S_5] - P_r[S_4]| \leq q_{hash} \text{Adv}_G^{\text{ECDHP}} \quad (21)$$

GAME G_{a6} : In this game, if $\mathcal{U}_{A_{adv}}$ asks a hash query for abP then test query will be terminated.

The probability of obtaining the session key here is $q_{hash}^2/2^{l+1}$, So $\mathcal{U}_{A_{adv}}$ has no advantage in G_{a6} . The resultant of all equations that we got is:

$$\text{Adv}_{P_p}^{\text{AKA}} \leq \frac{q_{hash}^2}{2^{l-1}} + \frac{q_{send}}{2^{l-2}} + \frac{(q_{send} + q_{exe})^2}{p^2} + \frac{(q_{send} + q_{exe})^2}{p} + 2_{q_{hash}} \text{Adv}_G^{\text{ECDHP}} \quad (22)$$

8. Functionality Comparison and Performance Analysis

In this section, we compared our proposed scheme with related schemes [67–73] in terms of resource utilization (storage, communication, and computation cost) and security functionality. The detailed description is as follows.

8.1. *Computational Overhead Comparison.* We have evaluated our scheme and related schemes to determine the computational efficiency. For this purpose, we have considered hash function $h(\cdot)$ and point multiplication PM. Cryptographic operations have been implemented at the server end on a desktop device, whereas operations at U_i end are

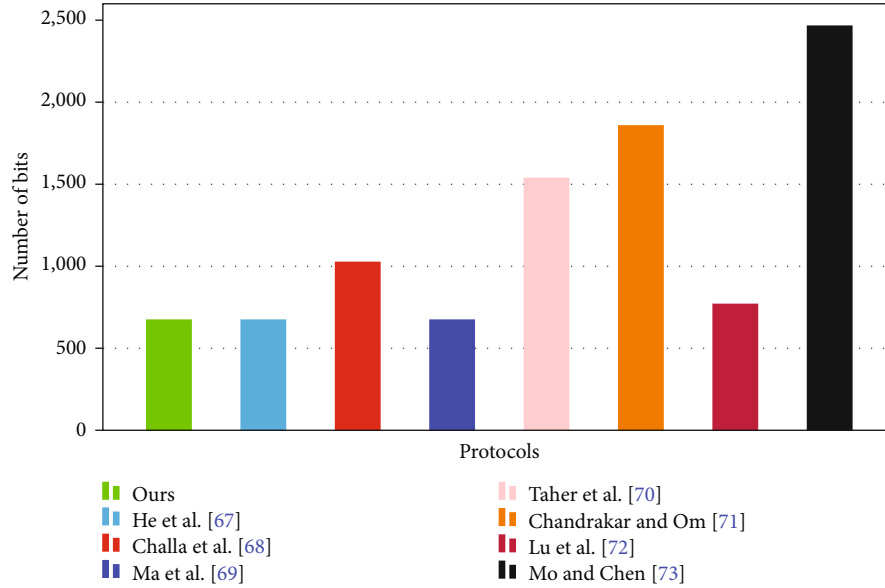


FIGURE 6: Comparison of the proposed and related scheme storage overhead.

implemented using a mobile device. The specifications of both devices are listed in Tables 2 and 3.

The time taken by hash and point multiplication on the system is 0.001032 and 0.002672 milliseconds (ms), respectively, whereas the time taken by hash and point multiplication on the system is 4 and 8 milliseconds (ms), respectively. The computation cost of the related and proposed schemes [67–73] is presented in Table 4. Table 4 shows that the proposed scheme requires 44.0094 ms for computation. The time required by [67–73] is also mentioned in Table 4.

If we present the Table 4 results graphically we can observe the proposed scheme is efficient in terms of computation as compared to [67, 68, 71–73] and slightly greater than [69, 70].

In Figure 4, the vertical axis (Y -axis) shows the time required in millisecond (ms), whereas schemes are presented on horizontal axis (X -axis). Figure 4 visually demonstrates the total time taken for the computation of the operations.

8.2. Communicational Overhead Comparison. We compared our proposed scheme with the related schemes [67–73] in terms of communicational expenses in this subsection. The communication structure of the proposed and related schemes [67–73] is demonstrated in Table 5 on the basis of scheme architecture. The communication structure in Table 5 shows the way in which communicating entities interact with each other and how they exchange messages. In Table 5, the symbol represents U_i : users, S_j : sensor node, TA: trusted authority, CS: server.

Considering the communication structure demonstrated the Table 5, we computed the communication cost as presented in Table 6. For conventional comparison, we assumed identities (ID_i , ID_{GWNs}), random numbers, and point multiplication require 160 bits respectively, whereas we assumed 256 bits for hash, secrete, and public keys (x , Pub). The total

bits required for communication by the proposed scheme is 2016 bits, whereas Table 6 shows the proposed scheme requires the least number of bits as compared to the related schemes [67–73].

The time taken for communication stated in Table 6 is graphically presented in Figure 5. The bits required for communication are displayed on the vertical axis (y -axis) and the schemes on the horizontal axis (x -axis). The proposed scheme requires less number of bits than [67–73] for communication.

8.3. Storage Overhead Comparison. The number of bits required to store parameters in smart devices (i.e., temper proof onboard memory/storage) is referred to as storage cost. In this subsection, we have compared our scheme with related schemes [67–73] for evaluating the storage efficiency. Table 7 depicts the storage cost comparison of proposed and related schemes. It is evident from the table that the proposed scheme’s storage cost is equal to [67] and less than [68–73].

The storage cost mentioned in Table 7 is graphically presented in Figure 6. In Figure 6, the vertical axis (y -axis) presents the number of bits, whereas the horizontal axis (x -axis) presents the schemes. Figure 6 clearly shows that the proposed scheme’s storage cost is less from [68–73] and equals to [67].

8.4. Security Functionality. In this subsection, we have discussed the proposed and related schemes in terms of security functionality. It is clear from Table 8 that the proposed scheme provides aided security as compared to related schemes.

Upon evaluating Tables 4, 6–8 we can state that the proposed scheme is efficient in terms of resource utilization; also, the proposed scheme provides aided and reliable security features. Thus, minimum resource utilization and enhanced

TABLE 8: Security features comparison of the proposed and related schemes.

Security features	Schemes							
	Ours	[67]	[68]	[69]	[70]	[71]	[72]	[73]
Mutual authentication	•	•	•	•	•	•	•	•
Key agreement	•	•	•	•	•	•	•	•
User Untraceability	•	◦	•	•	•	•	◦	•
User masquerading attack	•	•	•	•	•	•	◦	•
$\mathcal{E}\mathcal{W}\mathcal{N}$ masquerading attack	•	•	•	•	•	•	•	•
Man-in-middle attack (MITM)	•	•	•	•	•	•	•	•
Parallel session attack	•	•	•	≈	•	•	•	•
Privileged insider and stolen verifier attack	•	•	◦	•	•	•	◦	•
Perfect forward secrecy	•	•	•	•	•	•	◦	•
No clock synchronization	•	◦	◦	◦	◦	◦	◦	◦

• resists, ◦ not resists, ≈ not applicable.

security features make the proposed authentication scheme efficient and suitable for the underlying infrastructure.

9. Conclusion

We have proposed an identity-based three-party lightweight remote user authentication scheme, for an IoT environment. We have demonstrated with the help of informal security analysis that the proposed scheme does not let any attacker to penetrate the system. We have shown that the proposed scheme has a vigorous capability to resist various attacks. In addition, formal security proof of the proposed scheme is given using Real-Or-Random (ROR); it shows that there exists secure mutual authentication between the remote users through a gateway in IoT infrastructure. Furthermore, the storage, computation, and communication cost of our scheme is far less than various related schemes. Hence, our proposed scheme is more efficient and reliable for IoT infrastructure as compared to various existing schemes.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] S. Qu, L. Zhao, and Z. Xiong, "Cross-layer congestion control of wireless sensor networks based on fuzzy sliding mode control," *Neural Computing and Applications*, vol. 32, no. 17, pp. 13505–13520, 2020.
- [2] H. Chen, Y. Chen, and L. Yang, "Intelligent early structural health prognosis with nonlinear system identification for RFID signal analysis," *Computer Communications*, vol. 157, pp. 150–161, 2020.
- [3] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 4, pp. 1373–1384, 2006.
- [4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, 2006.
- [5] Z. Cheng, L. Chen, R. Comley, and Q. Tang, "Identity-based key agreement with unilateral identity privacy using pairings," in *International Conference on Information Security Practice and Experience*, pp. 202–213, Springer, Berlin, Heidelberg, 2006.
- [6] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC press, 1996.
- [7] J. Zhou and K.-Y. Lam, "Undeniable billing in mobile communication," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking - MobiCom '98*, Dallas, TX, USA, 1998.
- [8] Y. Liu and J. Cao, "An improved anonymous remote authentication protocol," in *2009 Second International Symposium on Information Science and Engineering*, pp. 181–184, Shanghai, China, 2009.
- [9] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in *European Symposium on Research in Computer Security*, pp. 277–293, Springer, 1998.
- [10] S.-J. Wang, "Anonymous wireless authentication on a portable cellular mobile system," *IEEE Transactions on Computers*, vol. 53, no. 10, pp. 1317–1329, 2004.
- [11] G. Horn, K. M. Martin, and C. J. Mitchell, "Authentication protocols for mobile network environment value-added services," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 2, pp. 383–392, 2002.
- [12] Z. Jia, Y. Zhang, H. Shao, Y. Lin, and J. Wang, "A remote user authentication scheme using bilinear pairings and ecc," in *Sixth International Conference on Intelligent Systems Design and Applications*, Jinan, China, 2006.
- [13] G. Shailaja, K. P. Kumar, and A. Saxena, "Pairing based mutual authentication scheme using smart cards," *IACR Cryptology ePrint Archive*, vol. 2006, p. 152, 2006.
- [14] Y.-P. Liao and S.-S. Wang, "A secure and efficient scheme of remote user authentication based on bilinear pairings," in *TENCON 2007 - 2007 IEEE Region 10 Conference*, Taipei, Taiwan, 2007.
- [15] C. Yang, W. Ma, and X. Wang, "Novel remote user authentication scheme using bilinear pairings," in *Lecture Notes in Computer Science*, pp. 306–312, Springer, Berlin, Heidelberg, 2007.

- [16] Y.-M. Tseng, T.-Y. Wu, and J.-D. Wu, "A mutual authentication and key exchange scheme from bilinear pairings for low power computing devices," in *31st Annual International Computer Software and Applications Conference - Vol. 2 - (COMP-SAC 2007)*, pp. 700–710, Beijing, China, 2007.
- [17] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*, pp. 47–53, Springer, Berlin, Heidelberg, 1984.
- [18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology — CRYPTO 2001*, pp. 213–229, Springer, Berlin, Heidelberg, 2001.
- [19] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, 2006.
- [20] M. Abdalla, D. Catalano, C. Chevalier, and D. Pointcheval, "Efficient two-party password-based key exchange protocols in the uc framework," in *Topics in Cryptology – CT-RSA 2008*, pp. 335–351, Springer, Berlin, Heidelberg, 2008.
- [21] C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterprise Information Systems*, pp. 1–16, 2020.
- [22] A. Irshad, M. Usman, S. Ashraf Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for Energy Internet based Vehicle-to-Grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, p. 1, 2020.
- [23] K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, S. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, p. 4752, 2019.
- [24] T.-Y. Chang, M.-S. Hwang, and W.-P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 181, no. 1, pp. 217–226, 2011.
- [25] H. Cheng and Y. Liu, "An improved RSU-based authentication scheme for VANET," *Journal of Internet of Technology*, vol. 21, no. 4, pp. 1137–1150, 2020.
- [26] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 8, pp. 3133–3142, 2019.
- [27] C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang, "An novel three-party authenticated key exchange protocol using one-time key," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 498–503, 2013.
- [28] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, "Security and key management in iot-based wireless sensor networks: an authentication protocol using symmetric key," *International Journal of Communication Systems*, vol. 32, no. 16, 2019.
- [29] Z. W. Tan, "A Note on an Enhanced Three-Party Authentication Key Exchange Protocol," *Key Engineering Materials*, vol. 439–440, pp. 1367–1372, 2010.
- [30] H. Wang, H. Zhang, J. Li, and C. Xu, "A (3, 3) visual cryptography scheme for authentication," *Journal of Shenyang Normal University*, vol. 31, no. 101, 2013.
- [31] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.
- [32] A. Alrawais, A. Althothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.
- [33] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, p. 19, 2017.
- [34] T. X. Tran, M.-P. Hosseini, and D. Pompili, "Mobile edge computing: recent efforts and five key research directions," *IEEE COMSOC MMTC Commun.-Frontiers*, vol. 12, pp. 29–34, 2017.
- [35] E. Ahmed and M. H. Rehmani, *Mobile Edge Computing: Opportunities, Solutions, and Challenges*, Elsevier, 2017.
- [36] J.-H. Yang and C.-C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computers & Security*, vol. 28, no. 3–4, pp. 138–143, 2009.
- [37] E.-J. Yoon and K.-Y. Yoo, "Robust ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC," in *2009 International Conference on Computational Science and Engineering*, Vancouver, BC, Canada, 2009.
- [38] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.
- [39] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Systems Journal*, vol. 9, no. 3, pp. 805–815, 2015.
- [40] Q. Jiang, J. Ma, and F. Wei, "On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Systems Journal*, vol. 12, no. 2, pp. 2039–2042, 2018.
- [41] A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, S. A. Chaudhry, and R. Kumar, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *TIIS*, vol. 10, no. 12, pp. 5529–5552, 2016.
- [42] R. Amin, S. H. Islam, G. Biswas, D. Giri, M. K. Khan, and N. Kumar, "A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments," *Security and Communication Networks*, vol. 9, no. 17, pp. 4650–4666, 2016.
- [43] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Future Generation Computer Systems*, vol. 62, pp. 190–195, 2016.
- [44] M. H. Ibrahim, "Octopus: an edge-fog mutual authentication scheme," *IJ Network Security*, vol. 18, no. 6, pp. 1089–1101, 2016.
- [45] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2052–2064, 2016.
- [46] L. Xiong, D. Peng, T. Peng, and H. Liang, "An Enhanced Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 12, 2017.
- [47] H. Zhu and S. Geng, "A three-party dynamic identity-based authenticated key exchange protocol with forward

- anonymity,” *Wireless Personal Communications*, vol. 109, no. 3, pp. 1911–1924, 2019.
- [48] K. Renuka, S. Kumar, S. Kumari, and C.-M. Chen, “Cryptanalysis and improvement of a privacy-preserving three-factor authentication protocol for wireless sensor networks,” *Sensors*, vol. 19, no. 21, p. 4625, 2019.
- [49] A. K. Das, “A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks,” *Wireless Personal Communications*, vol. 82, no. 3, pp. 1377–1404, 2015.
- [50] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, “Three party secure data transmission in iot networks through design of a lightweight authenticated key agreement scheme,” *Future Generation Computer Systems*, vol. 100, pp. 882–892, 2019.
- [51] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, “Authenticated key agreement scheme for fog-driven IoT healthcare system,” *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.
- [52] M. Ramadan, Y. Liao, F. Li, and S. Zhou, “Identity-based signature with server-aided verification scheme for 5G mobile systems,” *IEEE Access*, vol. 8, pp. 51810–51820, 2020.
- [53] S. Kumar, S. Akbar Abbas Jafri, N. A. Nigam, N. Gupta, G. Gupta, and S. K. Singh, “A new user identity based authentication, using security and distributed for cloud computing,” *IOP Conference Series: Materials Science and Engineering*, vol. 748, 2020.
- [54] N. Farjana, S. Roy, M. J. N. Mahi, and M. Whaiduzzaman, “An identity-based encryption scheme for data security in fog computing,” in *Proceedings of International Joint Conference on Computational Intelligence*, pp. 215–226, Dhaka, Bangladesh, 2020.
- [55] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, “Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets,” *IEEE Systems Journal*, pp. 1–11, 2020.
- [56] X. Jia, N. Hu, S. Su et al., “IRBA: an identity-based cross-domain authentication scheme for the internet of things,” *Electronics*, vol. 9, no. 4, p. 634, 2020.
- [57] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, “Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems,” *Computer Communications*, vol. 153, pp. 527–537, 2020.
- [58] S. Hussain and S. A. Chaudhry, “Comments on biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10936–10940, 2019.
- [59] M. Ramadan, Y. Liao, F. Li, S. Zhou, and H. Abdalla, “IBEET-RSA: identity-based encryption with equality test over RSA for wireless body area networks,” *Mobile Networks and Applications*, vol. 25, no. 1, pp. 223–233, 2020.
- [60] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, “Efficient and privacy-preserving authentication scheme for wireless body area networks,” *Journal of Information Security and Applications*, vol. 52, p. 102499, 2020.
- [61] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.
- [62] G. Hammouri, E. Öztürk, and B. Sunar, “A tamper-proof and lightweight authentication scheme,” *Pervasive and Mobile Computing*, vol. 4, no. 6, pp. 807–818, 2008.
- [63] M. N. Aman, K. C. Chua, and B. Sikdar, “Mutual authentication in IoT systems using physical unclonable functions,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327–1340, 2017.
- [64] M. Bellare, A. Desai, E. Jorjani, and P. Rogaway, “A concrete security treatment of symmetric encryption,” in *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pp. 394–403, Miami Beach, FL, USA, 1997.
- [65] M. Bellare, D. Pointcheval, and P. Rogaway, “Authenticated key exchange secure against dictionary attacks,” in *International conference on the theory and applications of cryptographic techniques*, pp. 139–155, Springer, Berlin, Heidelberg, 2000.
- [66] M. Abdalla, P.-A. Fouque, and D. Pointcheval, “Password-based authenticated key exchange in the three-party setting,” in *International Workshop on Public Key Cryptography*, pp. 65–84, Springer, Berlin, Heidelberg, 2005.
- [67] J. He, Z. Yang, J. Zhang, W. Liu, and C. Liu, “On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 14, no. 1, 2018.
- [68] S. Challa, M. Wazid, A. K. Das et al., “Secure signature-based authenticated key establishment scheme for future iot applications,” *IEEE Access*, vol. 5, pp. 3028–3043, 2017.
- [69] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, “An efficient and provably-secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.
- [70] B. H. Taher, S. Jiang, A. A. Yassin, and H. Lu, “Low-overhead remote user authentication protocol for iot based on a fuzzy extractor and feature extraction,” *IEEE Access*, vol. 7, pp. 148950–148966, 2019.
- [71] P. Chandrakar and H. Om, “A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC,” *Computer Communications*, vol. 110, pp. 26–34, 2017.
- [72] Y. Lu, G. Xu, L. Li, and Y. Yang, “Anonymous three-factor authenticated key agreement for wireless sensor networks,” *Wireless Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.
- [73] J. Mo and H. Chen, “A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks,” *Security and Communication Networks*, vol. 2019, Article ID 2136506, 17 pages, 2019.

Research Article

Offline/Online Outsourced Attribute-Based Encryption with Partial Policy Hidden for the Internet of Things

Xixi Yan, Guanghui He , Jinxia Yu, Yongli Tang , and Mingjie Zhao

School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, 454000 Henan, China

Correspondence should be addressed to Yongli Tang; yltang@hpu.edu.cn

Received 19 April 2020; Revised 9 July 2020; Accepted 31 July 2020; Published 4 September 2020

Academic Editor: Fei Yu

Copyright © 2020 Xixi Yan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the Internet of Things (IoT) environment, the intelligent devices collect and share large-scale sensitive personal data for a wide range of application. However, the power of storage and computing of IoT devices is limited, so the mass perceived data will be encrypted and transmitted to a cloud platform-interconnected IoT devices. Therefore, the concern how to save the encryption/decryption cost and preserve the privacy of the sensitive data in IoT environment is an issue that deserves research. To mitigate these issues, an offline/online attribute-based encryption scheme that supports partial policy hidden and outsourcing decryption will be proposed. This scheme adopts offline/online attribute-based encryption algorithms; then, the key generation algorithm and encryption algorithm are divided into two stages: offline stage and online stage. Meanwhile, in order to solve the problem of policy disclosure under the cloud platform, the policy hidden is supported, that is, the attribute is divided into the attribute value and the attribute name. For the pairing operation involved in decryption process, a verifiable outsourced decryption is implemented. Our scheme is constructed based on composite bilinear groups, which meets full security under the standard model. Finally, by comparing with other schemes in terms of functionality and computational overhead, it is shown that the proposed scheme is more efficient and applicable to the mobile devices with limited computing and storage functions in the Internet of Things environment.

1. Introduction

With the continuous development of the Internet of Things technology, it has been widely used in the fields of health care, smart home, industrial manufacturing, and environmental monitoring. But the computing and storage resources of Internet of Things equipment are often limited; an increasing number of individuals or organizations are outsourcing the storage of personal information to the cloud server to achieve lower cost. However, due to the cloud server being not completely trusted, therefore, how to protect the private information contained in the data and how to deal with the huge computing cost for the mobile devices with limited resources are the problems that should be solved in the current research.

In the application of intelligent medicine, personal health information records are collected through wearable devices (e.g., smart bracelets); then, it will be solved by a medical information integration platform. Personal Health Record

(PHR) is the core basic component of intelligent medical, which involves a lot of personal privacy information of users. The data need to be shared with relevant doctors, relatives, and friends, so it is important to achieve the fine-grained access control of data and related equipment. Sahai and Waters proposed a new public key cryptosystem called attribute-based encryption (ABE) [1]. Subsequently, it can be divided into two categories according to the location of the access policy: key policy attribute-based encryption (KP-ABE) [2] and ciphertext policy attribute-based encryption (CP-ABE) [3]. In CP-ABE schemes, access policy is embedded in ciphertext implicitly and outsourced to Cloud Service Provider (CSP) together with ciphertext in cloud environment. Because access policies are publicly available, everyone can access policies that contain some private information. For example, in the intelligent medical system, the patient authorized the cardiologist to access the encrypted data through the access policy as {Department: Cardiology; Doctor: Alice}. If anyone sees the encrypted data, it would

still be concluded that the patient obtained “heart disease” without decryption. If the content of the attribute value in the policy is not visible, that is, the policy is set as {Department: xxx; Doctor: xxx}, then the patient’s privacy can be guaranteed.

In order to avoid leaking the sensitive information implicit in the strategy, how to hide the access strategy has become a concern of many scholars. Nishide et al. [4] first proposed the ciphertext policy attribute-based encryption with hiding access structure. The implicit access structure in the ciphertext is not sent along with the ciphertext, that is, no one can obtain the access structure information. But the policy in the scheme only supports the “AND” gate structure. Lai et al. [5] proposed a CP-ABE with partial access structure hidden which achieved better policy expression. Different from the previous schemes, the attribute is divided into two parts: attribute name and attribute value. The attribute name can be publicized, while the attribute value is hidden. Li et al. [6] proposed an efficient attribute-based encryption scheme with partial hiding policy. The scheme has less decryption cost, but the public parameters, ciphertext, and attribute information related to the policy are easily obtained by arbitrary malicious users. Therefore, Yin et al. [7] proposed a more efficient scheme for the deficiency of Li et al.’s [6] scheme in the standard model. It is successfully reduced to the DBDH assumption. Cui et al. [8] constructed a scheme based on a composite order group supporting hidden attribute value, but it only achieves selective security. In the application scenario of the electronic medical system, Zhang et al. [9] not only implements the policy semiconcealment but also takes less computing cost and storage overhead during the decryption process. In addition, the scheme is fully secure under the standard model. However, the bilinear pairing operation and modular power operation involved in decryption process are still associated with numbers of attribute. For decreasing the complicate pairing operation, Hu et al. [10] proposed a semihiding attribute-based encryption scheme with constant pairing operation, but the modular power operation is still linearly related to the number of attributes. However, the above scheme only realizes access structure hidden, and the computing overhead relates to the complexity of access structure and the number of attributes; what is more, the process of encryption and decryption also needs a large number of modular power operation and pairing operation.

It is a fact that IoT devices need to be in real-time online when generating policy-related ciphertext, but the IoT devices with limited computing and storage are not always online. In order to solve this problem, Li et al. [11] put forward an offline/online attribute-based encryption supporting the access policy invisible. The key generation and encryption operation are divided into offline and online phases. That is to say, the key and ciphertext are precalculated in the offline phase, while a small amount of overhead is calculated to complete all the key components and ciphertext in the online phase. However, the pairing operation involved in decryption is still linearly related to the number of attributes required for decryption. In this paper, we propose an offline/online attribute-based encryption scheme which can

not only hide access structure but also support outsourcing decryption. The main contributions are as follows.

- (1) Partial access policy hidden: different from the technology of hiding access structure adopted by Li et al. [11], it divides attributes into two parts: attribute name and attribute value. Attribute name can be disclosed, and attribute value can be hidden. Hence, attribute name can be uploaded to cloud server provider (CSP) together with ciphertext, but attribute value is not visible
- (2) Outsourced decryption: in the decryption process, the bilinear pair operation and modular power operation are outsourced to the CSP for execution. The user only needs to verify the returned results and perform constant exponential operation to recover the plaintext
- (3) Fully secure: in this paper, our scheme is based on composite order groups and proved to be fully secure by the dual-system encryption technology [12]
- (4) Performance advantages: by comparing with the previous schemes from the aspects of function and performance, the proposed scheme has more advantages. And it is shown that our scheme is feasible in IoT by carrying out simulation experiments based on the PBC function library.

2. Related Work

2.1. Policy Hidden. In order to preserve the privacy of user attributes in the cloud environment, Nishide et al. [4] first proposed a CP-ABE scheme with access structure hidden. Lewko et al. [13] proposed a fully secure CP-ABE scheme by using a dual-system encryption technology under the standard model. Subsequently, Lewko and Waters [14] put forward a new proof method to achieve full security; however, the efficiency is lower. Lai et al. [5] and Jin et al. [15] gave a CP-ABE scheme supporting partial policy hidden. The scheme is proved to satisfy fully secure, but the access structure only support the “AND” gate structure. In order to reduce the bilinear pairwise operation and modular exponentiation involved in decryption process, the schemes [5, 16] gave the specific scheme. It is judged whether the attribute of users is matched with access policy before decryption first; if matched successfully, then the decryption operation is performed. But the scheme [16] only supports the “AND” gate structure, and the linear pair operation and modular exponentiation are still linearly related to the number of attributes during decryption period. At the same time, the scheme is proved to be selective secure, while Lai et al. [5] adopts more flexible LSSS structure, and the scheme is fully secure under the standard model. But the bilinear pairing operations and modular exponentiations involved in the user testing phase and the decryption phase increase linearly with the complexity of the policy. Yan et al. [17] introduced a multi-authority attribute-based encryption of partial policy hidden with dynamic policy updating. In the scheme, the policy

hiding is only to hide the attribute value, so it is called semi-hidden policy. The function of hidden attribute completely can also be realized by the inner product predicate encryption technology [18], but most of them only support the “AND” gate structure with weak expression ability, so there is a range of limitation in the actual application process.

2.2. Offline/Online Attribute-Based Encryption. The offline/online encryption, namely, preprocesses a lot of heavy work in the offline phase and responds to key requests or encryption tasks rapidly in the online phase. Even et al. [19] first proposed the offline/online digital signature technology. Liu et al. [20] gave an identity-based offline/online signature scheme in a wireless sensor network environment. Guo et al. [21] proposed an identity-based offline/online encryption scheme. Most of the computational work is pre-processed in the offline stage, and the actual encryption operation is completed in the online stage. Hohenberger and Waters [22] introduced an offline/online attribute-based encryption scheme in 2014, which is the first scheme that adopted the offline/online technology. Liu et al. [23] proposed a new ciphertext attribute-based encryption scheme by combining the offline/online technology and verification outsourcing technology. Wang et al. [24] proposed an offline/online attribute-based encryption scheme that achieved full security under the standard model. However, there was no verification of the part decryption results which is completed by cloud. Among existing intrusion prevention systems available, an industrial network intrusion detection algorithm is proposed based on the multifeatured data clustering optimization model [25]. With the development of electronic chip technologies of IoT, Liang et al. [26] introduced a fast deep reinforcement learning- (DRL-) based detection algorithm for virtual IP watermarks, by combining the technologies of mapping function and DRL to preprocess the ownership information of the IP circuit resource.

2.3. Outsourced Attribute-Based Encryption. Green et al. [27] proposed the first outsourced attribute-based encryption scheme which is secure in a random oracle model. The scheme commits the decryption operation to the decrypt server provider, so the ciphertext was converted into the type by ElGamal encryption, and then delivered to users so as to reduce computing cost of data user. Lai et al. [28] realized the outsourcing decryption and provided the accuracy verification of outsourcing calculation. Li et al. [29] presented an offline/online attribute-based encryption scheme, which will reduce the computational overhead during encryption phase with the offline/online technology. Also, the “chameleon” hash function was introduced to implement verification before the decryption phase. What is more, the scheme was proved to satisfy the adaptive chosen ciphertext attack security, but the bilinear pairing operation involved in decryption procession was still a large overhead for the user. Fan et al. [30] introduced a verifiable outsource scheme for multi-authorization in cloud-fog computing, which outsources encryption and decryption to fog nodes closed to the end user. Relative to the remote cloud sever provider, fog nodes can handle data with low latency, which was an ideal choice

for real-time calculation of data. Zhang et al. [31] proposed an access control of full outsourcing scheme for the first time, in which the key generation, encryption, and decryption operations are all handled by the cloud, but it lacks verification mechanism. Zhao et al. [32] put forward a verifiable full outsourcing scheme based on the original scheme [31]. The scheme supports verifiable and optimized performance that the computational cost does not increase significantly with the number of attributes or access policy complexity. Yu et al. [33] introduced a verifiable outsourced attribute-based encryption with partial policy hidden. In the particularity of blockchain-based industrial network, the data storage management faces enormous challenges. Liang et al. [34] focuses on data security issues in the industrial network and designs a storage and repair scheme for fault-tolerant data coding.

3. Preliminaries

3.1. Composite Order Bilinear Group. The proposed scheme is based on the composite order bilinear group whose order is the product of three distinct primes. Let Φ be an algorithm that inputs security parameter 1^λ and outputs a tuple $(p_1, p_2, p_3, G, G_T, e)$, where p_1, p_2, p_3 are 3 distinct primes, G, G_T are cycle groups of order $N = p_1 p_2 p_3$, and $e : G \times G \rightarrow G_T$ is a map function such that

(1) Bilinear:

$$\forall g, h \in G, a, b \in \mathbb{Z}_N, e(g^a, h^b) = e(g, h)^{ab} \quad (1)$$

(2) Nondegenerate: if $\exists g \in G$ such that the order of $e(g, g)$ is N in G_T .

Assuming that there is an group operation in G, G_T and the mapping function e , it is computable in polynomial time in λ . Let $G_{p_1}, G_{p_2}, G_{p_3}$ represent subgroups of G , the subgroups have order p_1, p_2, p_3 , respectively, then $G = G_{p_1} \times G_{p_2} \times G_{p_3}$. If $g_1 \in G_{p_1}, g_2 \in G_{p_2}$, then $e(g_1, g_2) = 1$. If the elements in the mapping function e are elements of different subgroups, the equation still hold; thus, the composite order bilinear group is said to satisfy its orthogonality.

3.2. Linear Secret Sharing Scheme (LSSS). The secret sharing scheme on the participant set P is called the linear secret sharing scheme if the following conditions are met.

- (1) A vector can be formed by the secret share of each party over \mathbb{Z}_p
- (2) For the secret sharing scheme Π , there is a matrix M of size $\ell \times n$ that maps each row of the matrix to an associated participant P . For $i = 1, \dots, \ell$, $\rho(i)$ is the party associated with the i -th row of M . We first generate a column vector $\mathbf{v} = (s, y_2, y_3, \dots, y_n)$, where $s \in \mathbb{Z}_p$ is a shared secret and r_i is randomly selected, $i = 2, \dots, n$. According to scheme Π , $M\mathbf{v}$ is ℓ secret shares of the shared secret s , which indicates $\lambda_i =$

$(Mv)_i$ is held the secret share by the participants $\rho(i)$.

The linear secret sharing scheme has the characteristics of linear reconstruction. If $S \in A$ is an access authorization set, then there is a constant $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ that let $\sum_{i \in I} \omega_i \lambda_i = s$ hold, where λ_i is the effective share of the secret s , $I = \{i : \rho(i) \in S\}$.

3.3. Key Derivation Function (KDF). KDF algorithm outputs bit string by inputting original secret key DK and length l . KDF algorithm is secure if it has following negligible advantage for adversary in any probability polynomial time.

$$|\Pr [\mathcal{A}(KDF(DK, l)) = 1] - \Pr [\mathcal{A}(\theta) = 1]|. \quad (2)$$

Note that $\theta \in \{0, 1\}^l$.

3.4. Complexity Assumption. The order of group G is defined as the product of three different prime numbers. For any nonempty set $Z \subseteq \{1, 2, 3\}$, the order of subgroup of group G is $\prod_{i \in Z} p_i$. In this paper, the subgroup is denoted by G_Z . The security is based on the following complexity assumptions, and a detailed description of the complexity assumptions is given.

$$\begin{aligned} G : (N = p_1 p_2 p_3, G, G_T, e) &\xleftarrow{R} \Phi, g_{Z_2} \xleftarrow{R} G_{Z_2}, \dots, g_{Z_k} \xleftarrow{R} G_{Z_k}, \\ D : (G, g_{Z_2}, \dots, g_{Z_k}), T_0 &\xleftarrow{R} G_{Z_0}, T_1 \xleftarrow{R} G_{Z_1}. \end{aligned} \quad (3)$$

Assumption 1. (The General Subgroup Decision Assumption): Given a group generation algorithm Φ , $Z_0, Z_1, Z_2, \dots, Z_k$ represent a nonempty subset of a set $\{1, 2, 3\}$, where Z_i satisfies $Z_0 \cap Z_i \neq \emptyset \neq Z_1 \cap Z_i$ or $Z_0 \cap Z_i = \emptyset = Z_1 \cap Z_i$, $i \geq 2$. Define the following distribution:

If the advantage of Adversary \mathcal{A} satisfies $Adv_{\Phi, \mathcal{A}}^1(\lambda) = |\Pr [\mathcal{A}(D, T_0) = 1] - \Pr [\mathcal{A}(D, T_1) = 1]|$, then this assumption can be broken.

$$\begin{aligned} G : (N = p_1 p_2 p_3, G, G_T, e) &\xleftarrow{R} \Phi, g_1 \xleftarrow{R} G_{p_1}, g_2, X_2, \\ Y_2 &\xleftarrow{R} G_{p_2}, g_3 \xleftarrow{R} G_{p_3}, \alpha, s \xleftarrow{R} \mathbb{Z}_N, \\ D : (G, g_1, g_2, g_3, g_1^\alpha X_2, g_1^s Y_2), T_0 &= e(g, g)^\alpha, T_1 \xleftarrow{R} G_T. \end{aligned} \quad (4)$$

Definition 2. For any probability polynomial time, if $Adv_{\Phi, \mathcal{A}}^1(\lambda)$ is a negligible function, then the algorithm meets Assumption 1.

Assumption 3. Given a group generation algorithm Φ , define the following distribution:

If the advantage of Adversary \mathcal{A} satisfies $Adv_{\Phi, \mathcal{A}}^2(\lambda) = |\Pr [\mathcal{A}(D, T_0) = 1] - \Pr [\mathcal{A}(D, T_1) = 1]|$, then this assumption can be broken.

Definition 4. For any probability polynomial time, if $Adv_{\Phi, \mathcal{A}}^2(\lambda)$ is a negligible function, then the algorithm meets Assumption 3.

4. System Algorithm and Security Model

4.1. Algorithm Definition. The algorithm included in this scheme is composed of the following seven algorithms:

Setup(λ, U) $\rightarrow PK, MSK$: the algorithm inputs the security parameters λ , attributes universe U , and outputs master key MSK and the public parameter PK including the Key Derivation Function (KDF)

Offline.KeyGen(PK, ς) $\rightarrow IK$: this algorithm is implemented by the attribute authority in the offline phase. Input the public parameter PK and attribute set ς , and return the intermediate key IK

Online.KeyGen(PK, MSK, IK, ς) $\rightarrow SK, TK$: this algorithm is implemented by the attribute authority in the online phase. It inputs the public parameter PK , master key MSK , attribute set ς , and intermediate key IK , then returns the transformed key TK and secret key SK , where TK is used for outsourced decryption and SK is used for user local decryption

Offline.Enc(PK, A) $\rightarrow IC$: the algorithm is run by the data owner in the offline stage. Input public parameters PK and access policy A ; it will output intermediate ciphertext IC

Online.Enc($PK, (M, \rho), IC, m$) $\rightarrow CT$: the algorithm is run by the data owner in the online stage. Input public parameters PK , intermediate ciphertext IC , and message m ; then, it outputs complete ciphertext CT

Transform_{out}(TK, CT) $\rightarrow CT'$: the algorithm is executed by the cloud server provider (CSP) to generate partial decryption ciphertext CT' by inputting the transformed key TK and the ciphertext CT

Decrypt(SK, CT, CT', PK) $\rightarrow m$: the algorithm is executed by the local user to generate m by inputting secret key SK , complete ciphertext CT , and partial decryption ciphertext CT' , then returns m .

4.2. Security Model. We define the security model of this paper through the security game between Challenger (Simulator) \mathcal{B} and Adversary \mathcal{A} . The game process is as follows:

Setup. Challenger \mathcal{B} performs the Setup algorithm and outputs the public parameter PK to the Adversary \mathcal{A}

Phase 1. Challenger \mathcal{B} initializes empty table T , empty set D , and integer $i = 0$. Adversary \mathcal{A} can repeatedly ask any of the following queries:

Create (ς). The challenger sets $i = i + 1$ run the key generation algorithm on the attribute set S to obtain the key set (SK, TK) , and finally stores (i, ς, SK, TK) in table T

Corrupt (x). If there is an x -th entity in table T , then the challenger obtains the entity (x, ς, SK, TK) and sets $D := D \cup \{\varsigma\}$, and then outputs the key set (SK, TK) to Adversary \mathcal{A} . If it does not exist, then outputs “ \perp ”

Challenge. For all $\zeta \in D, \zeta \notin A^*$, Adversary \mathcal{A} submits two equal-length messages m_0^*, m_1^* and access structures A^* to \mathcal{B} , the Challenger \mathcal{B} selects $b \in \{0, 1\}$ and encrypts the messages m_b in the access structure A^* , then sends the generated ciphertext CT^* to the Adversary \mathcal{A} .

Phase 2. The Challenger \mathcal{B} continues to respond to the adversary's queries in the way of *Phase 1*, but the adversary cannot ask the challenger the attribute set ζ that satisfies the policy A^* .

Guess. The Adversary \mathcal{A} outputs the guess value $b' \in \{0, 1\}$, and if $b' = b$, then the Adversary \mathcal{A} wins the game.

5. Our Construction

The offline/online attribute-based encryption scheme which supports the partial policy hidden and outsourced decryption proposed in this paper is inspired based on references [14, 24] and consists of the following seven algorithms. The scheme is constructed as follows:

Setup(λ, U) $\rightarrow PK, MSK$: the algorithm inputs the security parameters λ , attributes universe U , and selects a linear group G of order $N = p_1 p_2 p_3$, where $U = \mathbb{Z}_N, p_1, p_2, p_3$ are three different prime numbers, and p_i represents the order of subgroup G_{p_i} . Then, it randomly selects $\alpha, a, k, u, r \in \mathbb{Z}_N$ and $g \in G_{p_1}$, meanwhile setting the key derivation function KDF with the output length l and the resistant-collision hash function $H: \{0, 1\}^* \rightarrow \mathbb{Z}_N$, and finally outputs the public parameters $PK = (N, g, g^a, g^k, e(g, g)^\alpha, u, r, KDF, l, H)$ and the master key $MSK = (g^\alpha, g_3 \in G_{p_3})$.

The user attribute set is defined as $\zeta = (\chi_S, S)$, where χ_S represents the attribute name index, $\chi_S \subseteq \mathbb{Z}_N$, and $S = \{s_i\}_{i \in \chi_S}$ represents the attribute value set

Offline.KeyGen(PK, ζ) $\rightarrow IK$: the algorithm selects $t' \in \mathbb{Z}_N$ and calculates $K'_i = (g^{s_i})^{t'}$, where $i \in \chi_S$, then outputs $IK = (\{K'_i\}_{i \in \chi_S}, t')$

Online.KeyGen(PK, MSK, IK, ζ) $\rightarrow SK, TK$: it randomly selects $h, z \in \mathbb{Z}_N, R, R', R'', \{R_i\}_{i \in \chi_S} \in G_{p_3}$ and calculates $\tilde{K} = g^\alpha g^{at} g^{hk} R, \tilde{K}' = g^h R', \tilde{K}'' = g^t R'', \tilde{K}_i = K'_i$ then outputs the transformed key $TK = (K = \tilde{K}^{1/z} = g^{(\alpha+at+hk)/z} R^{1/z}, K' = \tilde{K}'^{1/z} = g^{h/z} R'^{1/z}, K'' = \tilde{K}''^{1/z} = g^{t'/z} R''^{1/z}, K_i = \tilde{K}_i = g^{s_i t'/z})$ and user secret key $SK = (z, TK)$.

Offline.Enc(PK, A) $\rightarrow IC$: the algorithm inputs the specified access policy $A = (M, \rho, \Psi)$, where M is a matrix of $\ell \times n$ and ρ is a function that maps the x -th row of the matrix M_x to the attribute name index. And $\Psi = (t_{\rho(1)}, t_{\rho(2)}, \dots, t_{\rho(\ell)}) \in \mathbb{Z}_N^\ell$ is the attribute value set associated with access policy (M, ρ) . Then, it selects a vector $v = (s, v_1, v_2, \dots, v_n), r_x \in_R \mathbb{Z}_N$, computes $key = e(g, g)^{\alpha s}, C = g^s, C'' = (g^k)^s, \{C_{1,x} = g^{\alpha \cdot M_x \cdot v} (g^{t_{\rho(x)}})^{-r_x}, D_{1,x} = g^{r_x}\}_{x \in [1, \ell]}$, and finally generates intermediate ciphertext $IC = (key, (M, \rho), C, C'' \{C_{1,x}, D_{1,x}\}_{x \in [1, \ell]})$

Online.Enc(PK, IC, m) $\rightarrow CT$: it firstly computes $C' = m \cdot key$. Next, it selects $t \in G_T$ and computes $\bar{C} = t \oplus KDF(key, l), \bar{C} = u^{H(m)} r^{H(t)}$, then finally outputs the complete ciphertext $CT = ((M, \rho), C, C', C'', \{C_{1,x}, D_{1,x}\}_{i \in [1, \ell]}, \bar{C}, \bar{C})$

*Transform*_{out}(TK, CT) $\rightarrow CT'$: after receiving the transformed key TK and the ciphertext CT , if the attribute set ζ satisfies access policy A , there is a subset $\chi \in I_{(M, \rho)}$ that satisfies $\{\rho(i) \mid i \in \chi\} \subseteq \chi_S$, where $I_{(M, \rho)} \subseteq \{1, 2, \dots, \ell\}$ denotes the subset of $\{1, 2, \dots, \ell\}$ that meets (M, ρ) , and then there exists a set of constants $\{\omega_i\}_{i \in \chi}$ such that $\sum_{i \in \chi} \omega_i \lambda_i = s$ holds, and λ_i is the valid share of the secret s . The procedure of transformed ciphertext $CT'_{transform}$ follows the steps below:

$$CT'_{transform} = \frac{e(C, K) e(C', K')}{\prod_{i \in \chi} \left(e(C_{1,i}, K'') e(D_{1,i}, K_{\rho(i)}) \right)^{\omega_i}} = e(g, g)^{\alpha s/z}. \quad (5)$$

which finally gain the partial decryption ciphertext $CT' = (CT'_{transform}, C', \bar{C}' = \bar{C}, \bar{C}' = \bar{C})$

Decrypt(SK, CT, CT', PK) $\rightarrow m$: the algorithm is run by data user, which takes $CT' = (CT'_{transform}, C', \bar{C}' = \bar{C}, \bar{C}' = \bar{C})$ and SK as input, then computes $key = C/CT'_{transform} = e(g, g)^{\alpha s}, m \leftarrow C/key$. If $\bar{C} \oplus KDF(key, l) \rightarrow t$ and $\bar{C}' = u^{H(m)} r^{H(t)}$ hold, meanwhile if $b = 1$, it outputs m , else $b = 0$, then returns "⊥."

6. Security Proof

$$K = \left((g_1^\alpha X_2) g_1^{at+hk} \right)^{1/z} R^{1/z} g_2^{t'/z}, K' = g_1^{h/z} R'^{1/z} g_2^{t'/z}, K'' = g_1^{t'/z} R''^{1/z}, K_i = g^{s_i t'/z} R_i^{1/z}. \quad (6)$$

Theorem 5. *If the Assumption 1 and Assumption 3 hold, then the proposed scheme based on the defined security model is fully secure and satisfies CPA (Chosen-Plaintext Attack) security.*

Proof. The security proof of the scheme is similar to that in literature [14], that is, the dual-system encryption technology is used to prove its security. First, define two semifunctional structures: semifunctional ciphertext and semifunctional key. The normal secret key can decrypt normal ciphertext and semifunctional ciphertext, but the semifunctional secret key cannot decrypt semifunctional ciphertext. And semifunctional key and semifunctional ciphertext are only used in security proof and do not appear in actual systems.

Semifunctional key: it first calls the normal key generation algorithm to generate a normal key $K, K', K'', \{K_i\}_{i \in \chi_S}$ and then randomly selects elements $\eta, \eta' \in G_{p_2}$ to generate a semifunctional key: $K\eta, K'\eta', K'', \{K_i\}_{i \in \chi_S}$; in other words, except for K, K' , the remaining components are multiplied by the elements in G_{p_2} .

Semifunctional ciphertext: first call the normal encryption algorithm to generate a normal ciphertext: $C, C', C'', \{C_{1,x}, D_{1,x}\}_{x \in [1, \ell]}$, then select a random exponent $a', k', s' \in \mathbb{Z}_N$, and random vector $\omega \in \mathbb{Z}_N$, where s' is the first element

in the set, random exponent $\eta_i, \gamma_x \in \mathbb{Z}_N$, then the semifunctional ciphertext is $C, C'g_2^s, C''g_2^{s'k'}, \{C_{1,x}g_2^{a'M_x\omega}g_2^{-\eta_{\rho(x)}\gamma_x}, D_{1,x}g_2^{\gamma_x}\}_{x \in [1,\ell]}$. The element structure in group G_{p_2} here is similar to the element structure in G_{p_1} , but not related to public parameters.

First, let Q denote the total number of key queries made by the adversary, and define the game $Game_k$, where $k \in [0, Q]$.

$Game_k$: in this game, the ciphertext obtained by to the attacker is a semifunctional ciphertext, the first k keys are also semifunctional, and the remaining keys are normal.

The security proof of the scheme based on Assumption 1 and Assumption 3 is demonstrated through a series of games. We first transition from $Game_{real}$ to $Game_0$, then to $Game_1$, and until to $Game_Q$, where the key and ciphertext submitted to the attacker are semifunctional. Finally, to $Game_{final}$ stop, the ciphertext obtained by to the attacker at this time is generated by semifunctional encryption of random messages. Because the attacker does not have any advantages in the final game, the security proof of the scheme in this paper ends here.

Lemma 6. *Under Assumption 1 (the general subgroup decision assumption), no polynomial time attacker can achieve a nonnegligible difference in advantage between $Game_{real}$ and $Game_0$.*

Proof. We first create an algorithm \mathcal{B} in probabilistic polynomial time to break the general subgroup decision assumption and set $Z_0 := \{1\}, Z_1 := \{1, 2\}, Z_2 := \{1\}, Z_3 := \{3\}$. Let g_1, g_3, T input to Algorithm \mathcal{B} , where g_1 is the generator of the group G_{p_1} , g_3 is the generator of the group G_{p_3} , and T is the random element of the group G_{p_1} or the random element of the group $G_{p_1 p_2}$. \mathcal{B} can act as a simulator to interact with the adversary, and \mathcal{B} can simulate or interact with the Adversary \mathcal{A} , depending on the nature of T .

\mathcal{B} chooses a random exponent $\alpha, a, k \in \mathbb{Z}_N$ and sets public parameters $PK = (N, g = g_1, g^a = g_1^a, g^k = g_1^k, e(g, g)^\alpha = e(g_1, g_1)^\alpha, u, r, KDF, l, H)$ to submit PK to Adversary \mathcal{A} . We notice that Simulator \mathcal{B} knows the master key MSK . When \mathcal{A} makes a secret key query, \mathcal{B} will call the normal key generation algorithm to create a secret key.

The adversary requests a challenge ciphertext and message related to the access policy $A = (\mathbf{M}, \rho, \Psi)$. \mathcal{B} randomly selects bit b and generates the ciphertext m_b ; then, g^s of implicit setting is equivalent to the part of G_{p_1} in T . \mathcal{B} randomly selects the vector $\tilde{v} \in \mathbb{Z}_N^n$, and the first element of the vector has a value of 1. At the same time, let $v = s\tilde{v}$ and select $r_x \in \mathbb{Z}_N, x \in [1, \ell]$ randomly, then set $r_x = s\tilde{r}_x$. We should note that the elements s, v, r_x are distributed randomly, and then, the corresponding ciphertexts are $C = T, C' = m_b \cdot e(g_1, T)^\alpha, C'' = T^k, C_{1,x} = T^{a \cdot M_x \cdot \tilde{v}} T^{-\tilde{r}_x \eta_{\rho(x)}}, D_{1,x} = T^{\tilde{r}_x}$.

If $T \in G_{p_1}$, the ciphertext is normal ciphertext, and \mathcal{B} simulates the game $Game_{real}$ and interacts with \mathcal{A} . If $T \in G_{p_1 p_2}$, it is a semifunctional ciphertext. And the elements in G_{p_2} are set as follows: g^s is the components of G_{p_2} in T, k'

is equivalent to the value of $k \bmod p_2, a'$ is equivalent to $a \bmod p_2, \omega$ is equivalent to $s\tilde{v} \bmod p_2, \eta_{\rho(x)}$ is equivalent to $t_{\rho(x)} \bmod p_2$, and γ_x is equivalent to $s'\tilde{r} \bmod p_2$. We note that these values are generated by proper distribution, and the values of the element $\bmod p_1, p_2$ uniformly selected at random $\bmod N$ are independently and uniformly distributed. We also notice that public parameters will leak the value of $a, k \bmod p_1$, so when $T \in G_{p_1 p_2}, \mathcal{B}$ and \mathcal{A} simulate game $Game_0$, and then \mathcal{B} can use adversary's nonnegligible distinction in these games to obtain a nonnegligible advantage to break Assumption 1 (general subgroup decision assumption).

Lemma 7. *Under Assumption 1 (the general subgroup decision assumption), no polynomial time attacker can achieve a nonnegligible difference in advantage between $Game_{k-1}$ and $Game_k$.*

Proof. We first create an algorithm \mathcal{B} in probabilistic polynomial time to break the general subgroup decision assumption and set $Z_0 := \{1, 3\}, Z_1 := \{1, 2, 3\}, Z_2 := \{1\}g, Z_3 := \{3\}, Z_4 := \{1, 2\}, Z_5 := \{2, 3\}$. Let $g_1, g_3, X_1 X_2, Y_2 Y_3, T$ input to Algorithm \mathcal{B} , where g_1, X_1 is the generator of the group G_{p_1}, X_2, Y_2 is the generator of the group G_{p_2}, g_3, Y_3 is the generator of the group G_{p_3} , and T is the random element of the group G_{p_1} or the random element of the group $G_{p_1 p_2 p_3}$. And \mathcal{B} can simulate $Game_{k-1}$ or $Game_k$ to interact with Adversary \mathcal{A} , depending on the nature of T .

\mathcal{B} chooses a random exponent $\alpha, a, k \in \mathbb{Z}_N$ and sets public parameters $PK = (N, g = g_1, g^a = g_1^a, g^k = g_1^k, e(g, g)^\alpha = e(g_1, g_1)^\alpha, u, r, KDF, l, H)$ to submit PK to Adversary \mathcal{A} . We noticed that Simulator \mathcal{B} knows the master key MSK . When \mathcal{A} makes a secret key request, \mathcal{B} will call the normal key generation algorithm to create a private key in response to \mathcal{A} 's key query. In response to the first $k-1$ key query of a, \mathcal{B} generates a semifunctional key according to the following. First, the normal key generation algorithm is called to generate the normal key $K, K', K'', \{K_i\}_{i \in \chi_s}$, and then the random value τ, τ' is selected to generate the semifunctional key: $K(Y_2 Y_3)^\tau, K'(Y_2 Y_3)^{\tau'}, K'', \{K_i\}_{i \in \chi_s}$, where group elements $Y_2^\tau, Y_2^{\tau'}$ are distributed uniformly and randomly in G_{p_2} .

In order to generate semifunctional challenge ciphertext, the adversary requests a challenge ciphertext and message m_0, m_1 related to access policy $A = (\mathbf{M}, \rho, \Psi)$. \mathcal{B} randomly selects bit b and generates the ciphertext of m_b , and the g^s is equivalent to the part of G_{p_1} in T . \mathcal{B} randomly selects the vector $\tilde{v} \in \mathbb{Z}_N^n$ and the first element value of the vector is 1, and set $g^s = X_1, v = s\tilde{v}, g^{r_x} = X_1^{\tilde{r}_x}$; then, the corresponding ciphertext calculated is as follows: $C = X_1 X_2, C' = m_b \cdot e(g_1, X_1 X_2)^\alpha, C'' = (X_1 X_2)^k, C_{1,x} = (X_1 X_2)^{a \cdot M_x \cdot \tilde{v}} (X_1 X_2)^{-\tilde{r}_x \eta_{\rho(x)}}, D_{1,x} = (X_1 X_2)^{\tilde{r}_x}$, where set $g_2^{s'} = X_2, k' = k \bmod p_2, a' = a \bmod p_2, \eta_{\rho(x)} = t_{\rho(x)} \bmod p_2, g_2^{r_x} = X_2^{\tilde{r}_x}$ implicitly. In order to create a semifunctional ciphertext, the value of $a, k \bmod$

p_2 will not be revealed by the public parameters. To generate the k -th key request query for the associated attribute set, \mathcal{B} randomly selects $t, z \in \mathbb{Z}_N$ and the random element $R, R', R'', \{R_i\} \in G_{p_3}$ and calculates the following components: $K = (g_1^{\alpha+at} T^k)^{1/z} R^{1/z}, K' = T^{1/z} R^{1/z}, K'' = g^{t/z} R''^{1/z}, K_i = g^{s_i t^{1/z}} R_i^{1/z}$.

If $T \in G_{p_1 p_3}$, the distributed key is a normal key. If $T \in G_{p_1 p_2 p_3}$, the distributed key is a semifunctional key, so when $T \in G_{p_1 p_3}$, \mathcal{B} simulates the game $Game_{k-1}$ to interact with adversary. When $T \in G_{p_1 p_2 p_3}$, \mathcal{B} simulates the game $Game_k$. Then, \mathcal{B} can take advantage of adversary's nonnegligible difference in these games to obtain a nonnegligible advantage to break Assumption 1 (general subgroup decision assumption).

Lemma 8. *Under Assumption 3 (the general subgroup decision assumption), no polynomial time attacker can achieve a nonnegligible difference in advantage between $Game_Q$ and $Game_{final}$.*

Proof. We first create an algorithm \mathcal{B} in probabilistic polynomial time to break the general subgroup decision Assumption 3. Let $g_1, g_2, g_3, g_1^\alpha X_2, g_1^s Y_2, T$ input to Algorithm \mathcal{B} , where T is the random element of $e(g_1, g_2)^{\text{as}}$ or the group G_T . And \mathcal{B} can simulate $Game_{k-1}$ or $Game_k$ to interact with the Adversary \mathcal{A} , depending on the nature of T .

\mathcal{B} chooses a random exponent $\alpha, a, k \in \mathbb{Z}_N$ and sets public parameters $PK = (N, g = g_1, g^\alpha = g_1^\alpha, g^k = g_1^k, e(g, g)^\alpha = e(g_1, g_1)^\alpha, u, r, KDF, l, H)$ to submit PK to Adversary \mathcal{A} . We noticed that Simulator \mathcal{B} knows the master key MSK . When \mathcal{A} generates the k -th key request query of the associated attribute set, \mathcal{B} randomly selects exponent $\alpha, a, k \in \mathbb{Z}_N$ and random elements $R, R', R'', \{R_i\} \in G_{p_3}$, then calculates the following components (see the formula (6)):

We note that the generated key is a semifunctional key. In response to the first $k - 1$ key query of a , \mathcal{B} generates a semifunctional key according to the following. First, the normal key generation algorithm is called to generate the normal key $K, K', K'', \{K_i\}_{i \in \mathcal{X}_S}$, and then, the random value τ, τ' is selected to generate the semifunctional key: $K(Y_2 Y_3)^\tau, K'(Y_2 Y_3)^{\tau'}, K'', \{K_i\}_{i \in \mathcal{X}_S}$, where group elements $Y_2^\tau, Y_2^{\tau'}$ are distributed uniformly and randomly in G_{p_2} .

To generate a semifunctional challenge ciphertext, \mathcal{B} randomly selects a vector $\tilde{v} \in \mathbb{Z}_N^n$, and the first element of the vector has a value of 1, while letting $v = s\tilde{v}$, randomly selects exponent $\tilde{r}_x \in \mathbb{Z}_N, x \in [1, \ell]$, and sets $r_x = s\tilde{r}_x$. We should note that the elements s, v, r_x are distributed randomly; then, the corresponding ciphertext is

$$\begin{aligned} C &= g_1^s Y_2, C' = m_b \cdot T, C'' = (g_1^s Y_2)^k, C_{1,x} \\ &= (g_1^s Y_2)^{a \cdot M_x \cdot \tilde{v} \cdot (-\tilde{r}_x) \cdot \eta_{\rho(x)}}, D_{1,x} = (g_1^s Y_2)^{\tilde{r}_x}. \end{aligned} \quad (7)$$

This ciphertext is a semifunctional ciphertext, where $g_2^{s'}$ is equivalent to Y_2 , a' is equivalent to $a \bmod p_2$, ω is equivalent to $s\tilde{v} \bmod p_2$, $\eta_{\rho(x)}$ is equivalent to $\text{tot}_{\rho(x)} \bmod p_2$, and $g_2^{r_x} = X_2^{\tilde{r}_x}$. These values are randomly distributed, because Y_2 are random elements in G_{p_2} , and the value of the $k, s_i, \tilde{r}_x, \tilde{v} \bmod p_2$ distributed is independent of the value of these elements $\bmod p_1$.

If $T = e(g_1, g_1)^{\text{as}}$, the generated ciphertext is a semifunctional ciphertext by encrypting m_b , and \mathcal{B} simulates the game $Game_Q$ and interacts with \mathcal{A} . If T is a random element in G_T , then it is a semifunctional ciphertext generated by encrypting a random message, \mathcal{B} simulation game $Game_{final}$. Therefore, \mathcal{B} can take advantage of \mathcal{A} 's nonnegligible difference in these games to obtain a nonnegligible advantage to break Assumption 3.

This completes proof of Theorem 5.

7. Performance Analysis

The proposed scheme is compared with the schemes [9, 11, 14, 22–24] from the perspectives of function and computing cost. In the comparison, G_{p_i} represents the subgroup of the order p_i , N indicates the number of attribute universe. $|\ell|$ represents the number of the matrix M row, and $|y|$ represents the number of attribute sets that satisfy the policy. We use E_G, E_{G_T} , and P to denote 1 module exponential time executed in G , a module exponential time executed in G_T , and 1 bilinear pair time executed, respectively. Because the main computing overhead of this scheme contains linear pairwise operation and modular exponentiation, module multiplication and hash operation can be ignored.

7.1. Theoretical Analysis. Table 1 mainly shows the comparison of the functionality of the scheme. It can be seen that Zhang et al. [9], Lewko and Waters [14], Wang et al. [24], and our scheme are constructed on the composite order group, and these schemes are proved to be fully secure, while the schemes of Li et al. [11], Waters et al. [22], and Liu et al. [23] do not achieve full security. In terms of attribute privacy protection, besides our scheme, Zhang et al. [9] and Li et al. [11] also implemented partial policy hidden. In terms of reducing computational overhead, Li et al. [11] and Waters et al. [22] adopt offline/online technology to solve the problem, while Liu et al. [23] and Wang et al. [24] not only adopt offline/online technology but also support outsourced decryption algorithms. However, the scheme of Liu et al. [23] supports the verification of outsourced decryption results, while the scheme of Wang et al. [24] does not implement verification mechanism. Based on the above analysis, the scheme proposed in this paper not only realizes the information hiding of attribute values but also adopts offline/online technology and verifiable outsourced decryption algorithms to reduce the user's local computational cost. Besides, it is proven to be fully secure.

Table 2 gives the analysis from the computing cost. Since the literatures [14, 22, 23] do not support the policy hidden function, no analysis and comparison are listed in Table 2.

TABLE 1: Comparison of performance.

Scheme	Policy hidden	Composite order	Fully secure	Offline/online key generation	Offline/online encryption	Outsourced decryption	Verify
Zhang et al. [9]	✓	✓	✓	✗	✗	✗	✗
Li [11]	✓	✗	✗	✓	✓	✗	✗
Lewko and Waters [14]	✗	✓	✓	✗	✗	✗	✗
Waters [22]	✗	✗	✗	✓	✓	✗	✗
Liu et al. [23]	✗	✗	✗	✓	✓	✓	✓
Wang et al. [24]	✗	✓	✓	✓	✓	✓	✗
Ours	✓	✓	✓	✓	✓	✓	✓

TABLE 2: Comparison of computing overhead.

Scheme	Offline encryption	Online encryption	Outsourced decryption	Local decryption
Zhang et al. [9]	—	$(6 \ell + 2)E_G + 2E_{G_T}$	—	$(2 y + 3)P + y E_G + y E_{G_T}$
Li [11]	$(4 \ell + 1)E_G + 1E_{G_T}$	$1E_G$	—	$(3 y + 2)P + (y + 1)E_G + y E_{G_T}$
Wang et al. [24]	$(3 \ell + 4)E_G + 1E_{G_T}$	0	$(3 y + 2)P + y E_G + y E_{G_T}$	$1E_G + 2E_{G_T}$
Ours	$(4 \ell + 3)E_G + 1E_{G_T}$	$2E_G$	$(2 y + 2)P + y E_{G_T}$	$2E_G + 1E_{G_T}$

It can be seen that the amount of computing required in the data encryption and data decryption stages is linearly and positively related to the number of attributes. The literatures [11, 24] and the proposed scheme use offline/online key generation and offline/online encryption technology. Therefore, most of the computing overhead in the data encryption process are performed in the offline phase, while it requires only a small amount of computing cost to complete key generation and data encryption operation in the online phase. In the scheme of [9], the modular exponentiation operation in the encryption process is much higher than other schemes. The literature [11] and our scheme have roughly the same modular exponentiation time. Although, the encryption cost of literature [24] is less than the $|\ell|$ modular exponentiation operation in literature [11] and our scheme. In the decryption process, our scheme is less than the $|y|$ linear pair operation and $|y|$ modular exponentiation operation in literature [24]. Compared with the scheme [11], our scheme is less than the $|y|$ linear pair operation and $(|y| + 1)$ modular exponentiation operation. Compared with the scheme [9], our scheme is less than the $|y|$ modular exponentiation operations. Therefore, the computational efficiency of our scheme is better than other related schemes.

7.2. Experiment Analysis. Through the above theoretical analysis, the proposed scheme has more advantages in term of function and efficiency. In order to evaluate the actual performance more accurately, we perform the experiment analysis. Because the literature [11] is based on prime order groups, and other schemes are based on composite order groups, for better comparison, we only analyze the time spent in literature [9] and literature [24] through simulation experiments, including the time required of offline encryption, online encryption, outsourced decryption, and local decryption.

Experimental environment: Windows 10, Inter® Core(TM) i5-8300H (2.30 GHz), memory 8GB, the experimental code is based on JPBC-2.0.0 (Java Pairing-Based Cryptography Library) function library and MyEclipse development environment. In the experiment, the paired structure of type A is used to construct an elliptic curve $y^2 = x^3 + x$ on a finite field. The order of the group is r , and the order of the base field is q . Here, we take $r = 160$ bit, $q = 512$ bit, where the pairing operation and modular exponent invoked `pairing.pairing(•)` and `G_1.powZn(•)` respectively, in the library for testing.

Experimental setup: in CP-ABE, the number of attributes in the access policy affects the encryption and decryption time. In the experiment process, we set the number of attributes as 20 and increase by 5 number of attributes each time, so it is tested with 4 different access policies. By comparing the computing time of the terminal user under different access policies, we can obtain the required time.

Figure 1 has four subfigures, Figures 1(a)–1(d), which represent the data owner’s offline encryption, online encryption time, cloud server decryption time required for outsourced partial decryption, and local user’s decryption time.

We can see in Figure 1(a) that the offline encryption time of our scheme is higher than the time of the literature [24]. In Figure 1(b), the online encryption process of the literature [24] does not involve modular exponentiation and pairing operation, so the computing time is 0, but compared with the literature [9], the encryption time of our scheme is constant, and its time of consumption is much lower than that of the literature [9]. In Figure 1(c), the decryption overhead performed by the cloud server is lower than that in the literature [24]. In Figure 1(d), the local decryption time of our scheme and that of the literature [24] are both constant, which is much lower than that of the scheme of literature

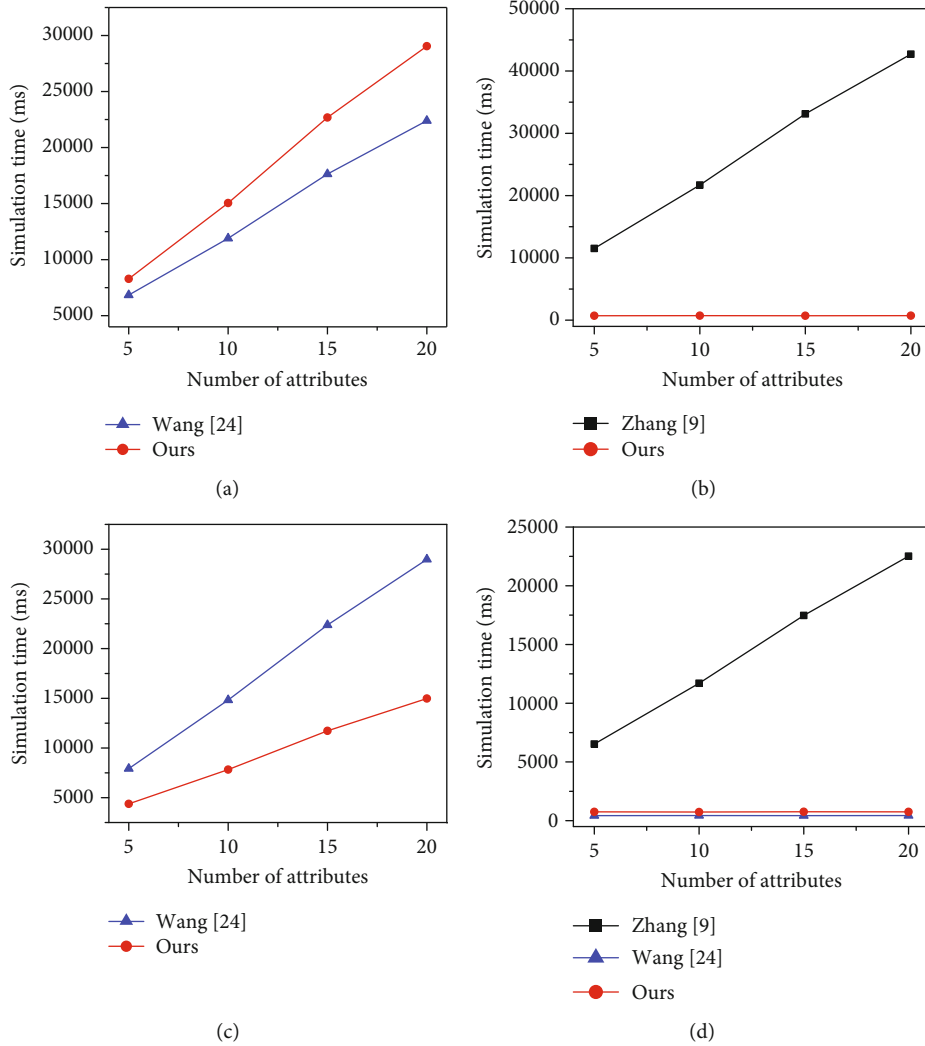


FIGURE 1: Simulation experiment. (a) Offline encryption. (b) Online encryption. (c) Outsourced decryption. (d) Local decryption.

[9]. The decryption time required is slightly higher than scheme of [24], but in [24], the partial decryption ciphertext returned by the cloud server is not supported verification; then, the correctness is not guaranteed. Meanwhile, Wang et al.'s scheme [24] cannot realize the policy hiding function. Since the proposed scheme supports outsourced decryption operations and verification operations, the user only needs to perform a constant number of exponential operations, which can not only reduce the user's calculation burden but also ensure the accuracy of partial decryption result returned.

From the above comprehensive analysis, the proposed scheme is superior to other schemes in terms of function and performance, so it is more effective and feasible in the IoT environment.

8. Conclusion

In order to solve the problem of privacy leaking and heavy computing overhead in IoT environment, an offline/online outsourced ABE scheme with partial policy hidden is pro-

posed in the paper. In the scheme, it divides attributes into two parts: attribute name and attribute value, attribute name is open and attribute value is hidden, to achieve the privacy of user attributes. Additionally, the offline/online technology is adopted to reduce the burden of encryption and decryption. A lot of heavy work can be preprocessed in the offline stage, and the rest computation only need to be done in the online stage. For the bilinear pairing operation and module power operation, the operation will be outsourced to the cloud server, and the user only needs to verify the outsourced calculation results to ensure the accuracy. It is proven that the scheme based on the static assumption problem can achieve full security under the standard model. Lastly, through theoretical and experiment analysis, it shows that our scheme has more advantages in the IoT environment.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Special Focus on Research and Promotion of Henan Province under Grant 192102210280, in part by the Research Foundation of Young Core Instructor in Henan Province under Grants 2018GGJS058 and 2019GGJS061, and in part by the Innovative Scientists and Technicians Team of Henan Provincial High Education under Grant 20IRTSTHN013.

References

- [1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Aarhus, Denmark, 2005.
- [2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, Alexandria, USA, 2006.
- [3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 321–334, Berkeley, USA, 2007.
- [4] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proceeding Application Cryptography Network Security (ACNS)*, pp. 13–23, Springer, 2009.
- [5] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 18–19, Seoul, South Korea, 2012.
- [6] J. Li, H. Wang, Y. Zhang, and J. Shen, "Ciphertext-policy attribute-based encryption with hidden access policy and testing," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 7, pp. 3339–3352, 2016.
- [7] H. Yin, L. Zhang, and Y. Cui, "Improving security in ciphertext-policy attributed-based encryption with hidden access policy and testing," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 7, pp. 3339–3352, 2016.
- [8] H. Cui, R. H. Deng, J. Lai, X. Yi, and S. Nepal, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited," *Computer Networks*, vol. 133, pp. 157–165, 2018.
- [9] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attributed-based access control," *IEEE internet of thing journal*, vol. 5, no. 3, pp. 1–15, 2018.
- [10] L. Zhang, G. Hu, Y. Mu, and F. Rezaeiabagha, "Hidden ciphertext policy Attribute-Based encryption with fast decryption for personal health record system," *IEEE Access*, vol. 7, pp. 33202–33213, 2019.
- [11] X. Li, H. Tian, and J. Ning, "Secure online/offline attribute-based encryption for IoT users in cloud computing," *International Conference on Provable Security*, pp. 347–354, 2019.
- [12] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumption," in *Annual International Cryptology Conference*, pp. 619–636, Santa Barbara, CA, USA, 2009.
- [13] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 62–91, 2010.
- [14] A. B. Lewko and B. Waters, "New proof methods for attribute-based encryption: achieving full security through selective techniques," *Annual Cryptology Conference*, 2012, pp. 180–198, Santa Barbara, CA, USA, August 2012.
- [15] C. Jin, X. Feng, and Q. Shen, "Fully secure hidden ciphertext policy attribute-based encryption with short ciphertext size," *Proceedings of the 6th International Conference on Communication and Network Security*, pp. 91–98, Singapore, 2016.
- [16] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42–61, 2017.
- [17] X. Yan, H. Ni, Y. Liu, and D. Han, "Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR," *Computer Science and Information Systems*, vol. 16, no. 3, pp. 831–847, 2019.
- [18] A. Lewko, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," *Annual international conference on the theory and applications of cryptographic techniques*, pp. 146–162, 2008.
- [19] S. Even, O. Goldreich, and S. Micali, "Online/offline digital signatures," *Proceedings of the Conference on the Theory and Application of Cryptology*, pp. 263–275, Santa Barbara, USA, 1989.
- [20] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287–296, 2010.
- [21] F. C. Guo, Y. Mu, and Z. D. Chen, "Identity-based online/offline encryption," *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 247–261, Cozumel, Mexico, 2008.
- [22] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," *Proceedings of the International Workshop on Public Key Cryptography*, pp. 293–310, Buenos Aires, Argentina, 2014.
- [23] Z. Liu, Z. L. Jiang, X. Wang, X. Huang, S. M. Yiu, and K. Sadakane, "Offline/online attribute-based encryption with verifiable outsourced decryption," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 7, pp. 1–17, 2017.
- [24] H. Wang, Z. Zheng, and Y. Wang, "Cloud-aided online/offline ciphertext-policy attribute based encryption in the standard model," *International Journal of Grid and Utility Computing*, vol. 8, no. 3, pp. 211–221, 2017.
- [25] W. Liang, K. C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2063–2071, 2020.
- [26] W. Liang, W. Huang, J. Long, K. Zhang, K. C. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6392–6401, 2020.

- [27] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," *Proceedings of the 20th USENIX Conference on Security*, pp. 1–16, San Francisco, USA, 2011.
- [28] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.
- [29] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.
- [30] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," *Sensors*, vol. 17, no. 7, pp. 1695–1710, 2017.
- [31] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," *Journal of Systems and Software*, vol. 125, no. 3, pp. 344–353, 2017.
- [32] Z. Y. Zhao, J. H. Wang, K. Y. Xu, and S. H. Guo, "Fully outsourced attribute-based encryption with verifiability for cloud storage," *Journal of Computer Research and Development*, vol. 56, no. 2, pp. 442–452, 2018.
- [33] J. Yu, G. He, X. Yan, Y. Tang, and R. Qin, "Outsourced ciphertext-policy attribute-based encryption with partial policy hidden," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, pp. 1–14, 2020.
- [34] W. Liang, Y. Fan, K. C. Li, D. Zhang, and J. L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 1–6552, 2020.

Research Article

Reversible Data Hiding for Encrypted 3D Model Based on Prediction Error Expansion

Li Li,¹ Shengxian Wang,^{1,2} Ting Luo ,³ Ching-Chun Chang,⁴ Qili Zhou,¹ and Hui Li²

¹Department of Computer Science, Hangzhou Dianzi University, Hangzhou 310018, China

²Key Laboratory of Brain Machine Collaborative Intelligence of Zhejiang Province, Hangzhou 310018, China

³College of Science and Technology, Ningbo University, Ningbo 315000, China

⁴Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

Correspondence should be addressed to Ting Luo; luoting@nbu.edu.cn

Received 11 June 2020; Revised 9 July 2020; Accepted 24 July 2020; Published 1 September 2020

Academic Editor: Fei Yu

Copyright © 2020 Li Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Since 3D models can intuitively display real-world information, there are potential scenarios in many application fields, such as architectural models and medical organ models. However, a 3D model shared through the internet can be easily obtained by an unauthorized user. In order to solve the security problem of 3D model in the cloud, a reversible data hiding method for encrypted 3D model based on prediction error expansion is proposed. In this method, the original 3D model is preprocessed, and the vertex of 3D model is encrypted by using the Paillier cryptosystem. In the cloud, in order to improve accuracy of data extraction, the dyeing method is designed to classify all vertices into the embedded set and the referenced set. After that, secret data is embedded by expanding direction of prediction error with direction vector. The prediction error of the vertex in the embedded set is computed by using the referenced set, and the direction vector is obtained according to the mapping table, which is designed to map several bits to a direction vector. Secret data can be extracted by comparing the angle between the direction of prediction error and direction vector, and the original model can be restored using the referenced set. Experiment results show that compared with the existing data hiding method for encrypted 3D model, the proposed method has higher data hiding capacity, and the accuracy of data extraction have improved. Moreover, the directly decrypted model has less distortion.

1. Introduction

With the rapid advancement of multimedia processing technologies on the internet, data hiding methods have been developed for the security of three-dimensional (3D) models [1–3]. Data hiding methods achieve integrity authentication and copyright protection by embedded secret data into the content of the original carrier [4, 5]. However, for the occasions with high data security requirement, such as medical images and judicial certification, no modification is allowed on the original carrier. Therefore, reversible data hiding (RDH) has attracted more researchers for potential applications [6–8].

Traditional RDH methods can be divided into three categories: difference expansion (DE), histogram shifting (HS),

and lossless compression (LC). DE-based RDH methods embed secret data into carrier image by expanding the difference among adjacent pixels [9, 10]. Prediction error expansion (PEE), which belongs to difference expansion, embeds secret data by expanding the difference between the actual value and the prediction value of pixels [11–14]. HS-based RDH methods generate the feature histogram of original image and embed secret data into the smallest point of the histogram [15, 16]. LS-based RDH methods compress the specified area of the carrier image and embed secret data into the compressed area [17].

With the development of outsourced storage in the cloud, reversible data hiding in encrypted domain (RDH-ED) has been studied for security of multimedia files in the cloud.

The existing RDH-ED methods are mainly classified into reserving room before encryption (RRBE) and vacating room after encryption (VRAE). The RRBE method reserves embedding room before encrypting the original image. For example, Ma et al. proposed a reversible data hiding method, in which the room is reversed by self-embedding before encryption. Zhang [19] constructed the histogram of prediction error and reserved room by HS, which is the most popular method for reversible data hiding. Cao et al. improved the method of [18, 19] by generating prediction error with a small entropy so that the reserved room can be increased, and the data hiding capacity can be improved [20].

The VRAE method directly implements data embedding by modifying the encrypted image [21, 22]. For example, Zhang embedded secret data by flipping the three least significant bits of a pixel [19]. With the help of the spatial correlation of natural images, the receiver extracted the secret data through the evaluation function of texture complexity. Based on the method of [19], Hong et al. increased data hiding capacity by improving the evaluation function [23]. Zhang [19] emptied out space for data embedding by using the typical manner of cipher-text compression.

However, the above RDH methods are for images and cannot be directly used to 3D models because the data structure of the 3D model is different from that of the image. Therefore, Wu and Cheung proposed a RDH method for 3D models based on DE, which embeds secret data by modifying the difference among adjacent vertices [24]. Jhou et al. constructed the histogram of the distance between all vertices and the center of 3D model and embedded secret data by histogram shifting. However, these methods cannot be implemented in the encrypted domain [25]. Jiang et al. proposed a RDH-ED method for 3D models based on stream cipher encryption [26]. By flipping several least significant bits of vertex coordinates, one bit was embedded. The receiver extracted secret data by using the spatial correlation of the original 3D model. Shah and Zhang proposed a watermarking method based on the Paillier cryptosystem, which used VRAE framework to vacate space before encryption [27]. Wang et al. embedded secret data in the encrypted domain by constructing direction histogram and histogram shifting [28].

Combining homomorphic encryption and prediction error expansion, a RDH method for encrypted 3D model is proposed in this paper. In this method, the original 3D model is preprocessed, and the vertex of 3D model is encrypted by using Paillier cryptosystem. In the cloud, in order to improve the accuracy of data extraction, the dyeing method is designed to classify all vertices into the embedded set and the referenced set. After that, the secret data is embedded by expanding direction of prediction error with direction vector. The prediction error of the vertex is computed by using the referenced set, and the direction vector is obtained according to the mapping table. Moreover, the mapping table is constructed to map several bits to a direction vector. Secret data can be extracted by comparing the angle between the direction of prediction error and direction vector, and the original model can be restored using the referenced set. The contributions of the paper are organized as follows.

- (1) By designing the dyeing method to classify all vertices into the embedded set and the referenced set, the error rate of data extraction can be reduced
- (2) The mapping table is constructed to map several bits to a direction vector, so that several bits can be embedded into a vertex, which improves data hiding capacity
- (3) Compared the existing RDH-ED methods, the proposed method has higher capacity, lower bit error rate, and the directly decrypted 3D model has less distortion

The rest of this paper is organized as follows. The Paillier cryptosystem is briefly introduced in Section 2. The related reversible data hiding method is proposed in Section 3. The experimental results are shown in Section 4. The conclusions are discussed in Section 5.

2. Related Algorithm

The Paillier cryptosystem [29], which has been widely used in encrypted signal processing, has homomorphism and probability. Homomorphism means that the product of two ciphertexts is consistent with the sum of two corresponding plaintexts. Probability means that different ciphertexts, which are obtained by encrypting the same plaintext with different parameters, can be decrypted to the same plaintext. The following describes the process of key generation, encryption, decryption, two characteristics, and subtraction homomorphism expansion.

2.1. Key Generation. Randomly pick up two large prime numbers p and q . Calculate $N = pq$ and $\lambda = \text{lcm}(p-1, q-1)$, where $\text{lcm}(\cdot)$ stands for the lowest common multiple. Afterwards, select $g \in Z_{N^2}^*$ randomly, which satisfies

$$\text{gcd}\left(L\left(g^\lambda \bmod N^2\right), N\right) = 1, \quad (1)$$

where $L(u) = (u-1)/N$, and $\text{gcd}(\cdot)$ means the greatest common divisor of two inputs. $Z_{N^2} = \{0, 1, 2, \dots, N^2 - 1\}$ and $Z_{N^2}^*$ are the numbers in Z_{N^2} which prime with N^2 . Finally, we get the public key (N, g) and corresponding private key λ .

2.2. Encryption. Select a parameter $r \in Z_{N^2}^*$ randomly. The plaintext $m \in Z_N$ can be encrypted to the corresponding ciphertext c by

$$c = E[m, r] = g^m \cdot r^N \bmod N^2, \quad (2)$$

where $E[\cdot]$ denotes the encryption function.

2.3. Decryption. The original plaintext m can be obtained by

$$m = D[c] = \frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N. \quad (3)$$

Moreover, two important characteristics are described as follows (which has been applied in the proposed method).

2.4. Lemma One. For two plaintexts $m_1, m_2 \in Z_N$, compute corresponding ciphertexts c_1, c_2 with r_1, r_2 according to Equation (1), respectively. The equation $c_1 = c_2$ holds if and only if $m_1 = m_2$ and $r_1 = r_2$.

2.5. Homomorphic Multiplication. For $\forall r_1, r_2 \in Z_N^*$, two plaintexts $m_1, m_2 \in Z_N$ and corresponding ciphertexts $E[m_1, r_1], E[m_2, r_2] \in Z_{N^2}^*$ satisfy

$$\begin{aligned} c_1 \cdot c_2 &= E[m_1, r_1] \cdot E[m_2, r_2] = g^{m_1+m_2} \cdot (r_1 \cdot r_2)^N \bmod N^2, \\ D[c_1 \cdot c_2] &= D[E[m_1, r_1] \cdot E[m_2, r_2] \bmod N^2] = m_1 + m_2 \bmod N. \end{aligned} \quad (4)$$

The original Paillier encryption system only has addition homomorphism and multiplication homomorphism. The subtraction homomorphism of the Paillier encryption system can be realized as follows.

2.6. Subtraction Homomorphic Expansion. In order to calculate the subtraction $m_1 - m_2$ of two numbers m_1, m_2 in the encrypted domain, the negative number $-m_2$ should be expressed by a positive number $N - m_2$. Suppose that $E[m_2]^{-1}$ denotes the ciphertext of $N - m_2$, the ciphertext $E[m_2]^{-1}$ can be calculated by Euclidean algorithm [30] and Modular Multiplication Inverse. Hence, the corresponding result of $m_1 - m_2$ in the encrypted domain can be obtained with $E[m_1] \cdot E[m_2]^{-1} \bmod N^2$.

3. The Proposed Reversible Data Hiding Method

In order to protect 3D model in the cloud, a reversible data hiding (RDH) method for encrypted 3D model is proposed. Figure 1 shows the flowchart of the proposed method. An original 3D model is preprocessed, and the vertex of 3D model is encrypted by using the Paillier cryptosystem. In the cloud, all vertices are classified into the embedded set and the referenced set. Then, the secret data is embedded by expanding direction of prediction error with direction vector. The prediction error of the vertex is computed by using the referenced set, and the direction vector is obtained according to the mapping table. Receiver can extract secret data by comparing the angle between prediction error and the direction vector, and the original model can be restored using the referenced set.

3.1. Preprocessing. Because the input of the Paillier cryptosystem should be a positive integer, the vertex coordinates firstly are converted from decimal to positive integer.

3D models are consisted of vertex data and connectivity data. The vertex data includes the coordinates of each vertex in the spatial domain. The connectivity data reflects the connection relationship between vertices. A 3D model Fairy and its local region are illustrated in Figure 2, and the corresponding format file is shown in Table 1. Each vertex and each face of the 3D model have a corresponding index, respectively. For a 3D model M , let $\{v_{ij}\}_{i=0}^{N_V}$ represent the sequence of vertices, where $v_i = (v_{ix}, v_{iy}, v_{iz})$, and N_V is the number of

vertices. Note that each coordinate $|v_{ij}| < 1, j \in \{x, y, z\}$, and the significant digit of each coordinate is 6.

Normally, uncompressed vertices are 32-bit floating point numbers with a precision of 6 digits. Therefore, the vertex coordinates are converted into an integer with k significant digits by using

$$v'_{i,j} = \lfloor v_{i,j} \cdot 10^k \rfloor, \quad j \in \{x, y, z\}. \quad (5)$$

Moreover, all vertex coordinates should be converted to positive integers for encryption by using

$$v'_{i,j} = v'_{i,j} + 10^k, \quad j \in \{x, y, z\}. \quad (6)$$

If k is greater than 6, the model can be restored losslessly; however, the time cost of encryption and decryption is large. If k is less than 6, the time cost is small, while the model cannot be restored losslessly. In order to balance the time cost and distortion of 3D model, the best k will be selected through the experiment.

3.2. Encryption. Referring to Equation (2), an integer r can be randomly selected to encrypt the vertex coordinates $v'_i = (v'_{ix}, v'_{iy}, v'_{iz})$ with the public key (N, g) .

$$c_{i,j} = E[v'_{i,j}, r_{i,j}] = g^{v'_{i,j}} r_{i,j}^N \bmod N^2, \quad j \in \{x, y, z\}, \quad (7)$$

where $c_{i,j}$ is the ciphertext from the plaintext $v'_{i,j}$.

3.3. Data Embedding. Firstly, the dyeing method is designed to classify all vertices into the embedded set and the referenced set. Secondly, the prediction error of the vertex in the embedded set is computed using the referenced set. Thirdly, a one-to-one mapping is constructed to map several bits to a direction vector. Finally, for embedding secret data, the direction vector and the embedded key are used to expand the direction of the prediction error. In addition, the embedded key is calculated to reduce the accuracy of data extraction.

3.3.1. Classifying the Vertices. For the vertex of 3D model, 1-ring neighborhood of the vertex refers to these vertices that are directly adjacent to the vertex. As shown in Figure 3, the vertex v'_j is adjacent of the vertex v'_i . If a vertex is modified to embed secret data, its 1-ring neighborhood cannot be modified, and it is mainly because the 1-ring neighborhood is required to calculate the prediction value of the vertex. Therefore, the dyeing algorithm is designed to classify all vertices into the embedded set and the referenced set because the color of adjacent vertices cannot be same. The vertices in the referenced set can be used to calculate the prediction value of the vertices in the embedded set because the referenced set consists of 1-ring neighborhood of all vertices in the embedded set, while the vertices in embedded set are modified to embed secret data.

Suppose that S_e denotes the embedded set, and S_r denotes the referenced set. In order to obtain large data hiding

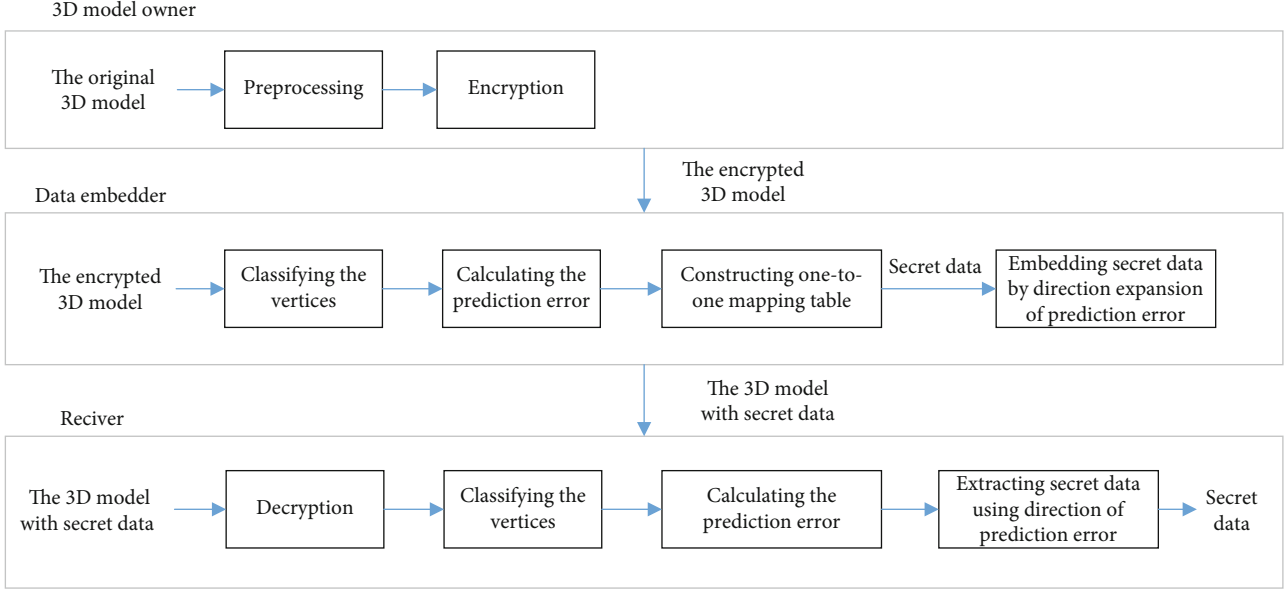


FIGURE 1: Flowchart of the proposed RDH-ED method.

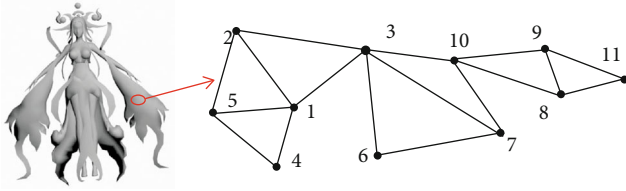


FIGURE 2: Illustration of a 3D model Fairy and its local region.

TABLE 1: File format of Figure 2.

Index of vertex	Vertex list			Face information	
	X-axis	Y-axis	Z-axis	Index of face	Elements in each face
1	$v_{1,x}$	$v_{1,y}$	$v_{1,z}$	1	(2,3,1)
2	$v_{2,x}$	$v_{2,y}$	$v_{2,z}$	2	(5,1,4)
3	$v_{3,x}$	$v_{3,y}$	$v_{3,z}$	3	(3,6,7)
4	$v_{4,x}$	$v_{4,y}$	$v_{4,z}$	4	(5,2,1)
5	$v_{5,x}$	$v_{5,y}$	$v_{5,z}$	5	(3,10,7)

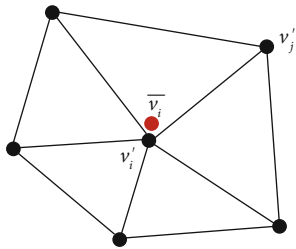


FIGURE 3: The actual value and the prediction value of the vertex.

capacity, the number of the vertices in the embedded set should be increased. The embedded set is the nonadjacent vertex set. According to graph theory, the existing polynomial algorithms can find the largest nonadjacent vertex set if the graph is a bipartite graph. However, the connectivity data of a 3D model cannot be represented by a bipartite graph since all loops of 3D model are 3. Hence, finding the largest embedded set in a 3D model is NP-hard problem. In order to increase data hiding capacity, the dyeing algorithm is designed to increase the number of the vertices in the embedded set.

Referring to the four-color theorem, different colors are required for any two adjacent vertices. For 3D models, at least seven colors are needed to dye the vertices to ensure that the colors of the adjacent vertices are different. After completing the process of dyeing, the color with most vertices is selected, and all vertices of this color are regarded as the embedded set, and the remaining vertices are regarded as the referenced set. Suppose that C denotes the color set of dyeing all vertices, Z_i denotes the color set of 1-ring neighborhood of the vertex, and c_i denotes the color of the i th vertex. The steps for the vertex classification using the dyeing algorithm are listed as follows.

Step 1. Suppose that the color of all vertices is black, and traverse all vertices in order of the vertex index.

Step 2. For an unclassified vertex v_i , statistic the color set of its 1-ring neighborhood.

Step 3. Dye the vertex v_i using the first color in C but not in Z_i .

Step 4. Determine whether the next vertex v_{i+1} is black. If v_{i+1} is black, the classification ends. If v_{i+1} is not black, loop from Step 2 until no vertex is black.

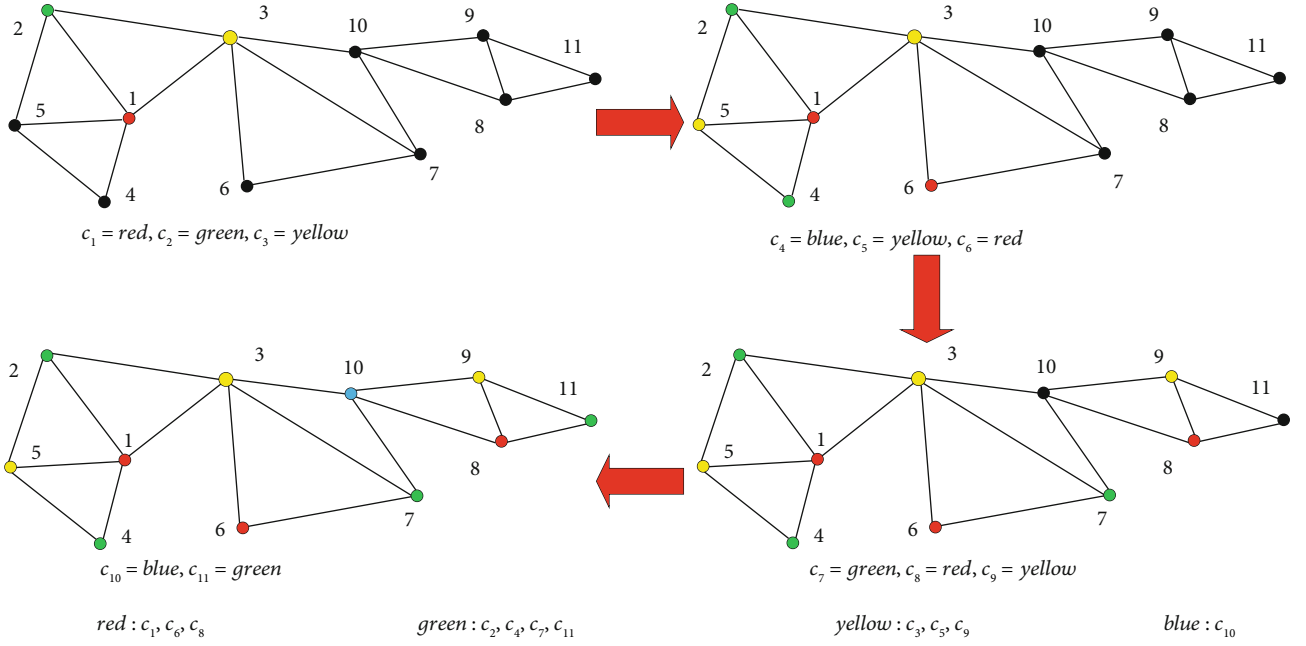


FIGURE 4: The process of classifying the vertices using the dyeing method.

TABLE 2: The one-to-one mapping table between weighted sum and direction vector.

Embed one bit into a vertex, which means $n = 1$, and $s_w \in [0, 1]$. On this condition, let $b_{k,j} \in \{-1, 1\}$.								
$s_w \in [0, 1]$	0	(-1,-1,-1)	1	(-1,-1,1)				
Embed two bits into a vertex, which means $n = 2$, and $s_w \in [0, 3]$. On this condition, let $b_{k,j} \in \{-1, 1\}$.								
$s_w \in [0, 3]$	0	(-1,-1,-1)	1	(-1,-1,1)	2	(-1,1,-1)	3	(-1,1,1)
Embed three bits into a vertex, which means $n = 3$, and $s_w \in [0, 7]$. On this condition, let $b_{k,j} \in \{-1, 1\}$.								
$s_w \in [0, 7]$	0	(-1,-1,-1)	1	(-1,-1,1)	2	(-1,1,-1)	3	(-1,1,1)
	4	(1,-1,-1)	5	(1,-1,1)	6	(1,1,-1)	7	(1,1,1)
Embed four bits into a vertex, which means $n = 3$, and $s_w \in [0, 15]$. On this condition, let $b_{k,j} \in \{-1, 0, 1\}$.								
$s_w \in [0, 15]$	0	(-1,-1,-1)	1	(-1,-1,0)	2	(-1,-1,1)	3	(-1,0,-1)
	4	(-1,0,0)	5	(-1,0,1)	6	(-1,1,-1)	7	(-1,1,0)
	8	(-1,1,1)	9	(0,-1,-1)	10	(0,-1,0)	11	(0,-1,1)
	12	(0,0,-1)	13	(0,0,1)	14	(0,1,-1)	15	(0,1,0)

Step 5. Select the most frequently used color, add all vertices of this color to the embedded set, and the remaining vertices are added to the referenced set.

Since all vertices are traversed only once, the time complexity of the dyeing algorithm is $O(n)$. For example, as illustrated in Figure 4, let $C = \{\text{red, green, yellow, blue}\}$. Traverse the vertex v_1 , and let $c_1 = \text{red}$ since $Z_1 = \{\text{black}\}$. Traverse the vertex v_2 , and let $c_2 = \text{green}$ since $Z_1 = \{\text{black, red}\}$. Traverse the vertex v_3 , and let $c_3 = \text{yellow}$ since $Z_1 = \{\text{black, red, green}\}$. After traversing all vertices, the most frequently used color green is selected. The vertex set $\{2, 6, 7, 11\}$ of color green is regarded as the embedded set, while the remaining vertices as the referenced set.

3.3.2. Computing of Prediction Error. The accuracy of prediction error directly affects the performance of data hiding. As shown in Figure 3, the vertex v'_j is adjacent to the vertex v'_i and the vertex \bar{v}_i is the prediction value of vertex v'_i . According to the correlation of adjacent vertices, prediction value \bar{v}_i can be calculated by using

$$\bar{v}_i = \frac{1}{N_i} \sum_{j=1}^{N_i} v'_j \quad j \in (1, N_i), \quad (8)$$

where N_i denotes the number of the adjacent vertices of the vertex v'_i .

The prediction error of the vertex v'_i can be calculated by using

$$\Delta v_i = v'_i - \bar{v}_i, \quad (9)$$

where Δv_i denotes the prediction error of the vertex v'_i . Δv_i is a three-dimensional vector with random direction. Due to the spatial correlation, the modulus length $|\Delta v_i|$ is usually small, and experiment results show that the modulus length $|\Delta v_i|$ has the maximum D . Hence, the range of $|\Delta v_i|$ is as follows.

$$|\Delta v_i| \in [0, D]. \quad (10)$$

3.3.3. Constructing the Mapping Table. In order to embed several bits into a vertex in the embedded set, several bits should be mapped to a direction vector.

Data embedder converts secret data into several groups with n bits, and n is a shared parameter. Let a group with n bits denote as $w(w_0, w_1, \dots, w_{n-1})$. Suppose that s_w denotes weighted sum of w , and s_w is calculated as

$$s_w = \sum_{i=0}^{n-1} w_i \cdot 2^i, \quad s_w \in [0, 2^n - 1]. \quad (11)$$

In order to embed s_w into a vertex, the corresponding direction vector of s_w should be constructed. Suppose that \vec{b}_{s_w} denotes the direction vector of s_w , and s_w is embedded by expanding the direction of prediction error with direction vector \vec{b}_{s_w} . The one-to-one mapping between weighted sum and direction vector is constructed as shown in Table 2. Let $b_{k,j} \in \{-1, 1\}$, $k \in [0, 7]$, and if $n \leq 3$, eight direction vectors can be constructed. The mapping between direction vector and weighted sum is shown at the top three rows in Table 2. Let $b_{k,j} \in \{-1, 0, 1\}$, $k \in [0, 26]$, and if $n = 4$, twenty-six direction vectors are constructed as shown at the fifth row in Table 2. Let $b_{k,j} \in \{-2, -1, 0, 1, 2\}$, $k \in [0, 110]$, and if $n = 5$ or $n = 6$, 110 direction vectors are constructed. Let W_{b_k} denote the direction weight of direction vector. As shown in Table 2, the direction vector \vec{b}_k is sorted according to the value W_{b_k} , and the direction weight W_{b_k} of the direction vector is calculated as follows.

$$W_{b_k} = 9b_{k,1} + 3b_{k,2} + b_{k,3}. \quad (12)$$

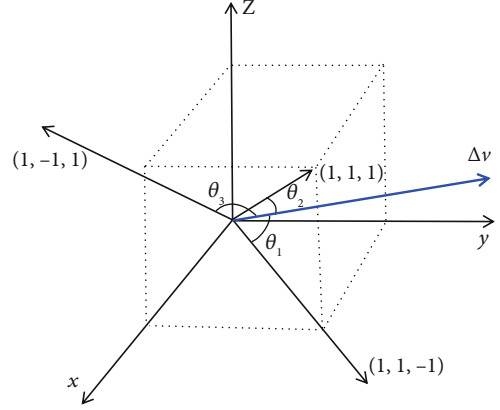


FIGURE 5: The angle between the prediction error and three direction vectors.

Hence, if the shared parameter n is obtained, the mapping table between weighted sum and direction vector can be constructed. For different s_w , the corresponding direction vector \vec{b}_{s_w} can be found through the mapping table.

For example, if $n = 2$, four direction vectors \vec{b}_{s_w} should be constructed to represent four weighted sum s_w , respectively. Let $b_{k,j} \in \{-1, 1\}$, eight direction vectors can be constructed, and the first four direction vectors are selected according to the direction weight W_{b_k} . As a result, the four direction vectors $(-1, -1, -1)$, $(-1, -1, 1)$, $(-1, 1, -1)$, and $(-1, 1, 1)$ are constructed to represent $s_w \in [0, 3]$, respectively.

3.3.4. Data Embedding. In order to embed secret data into the vertex, the vertex coordinates are required to be modified by using the direction vector and the embedding key. The weighted sum s_w of $w(w_0, w_1, \dots, w_{n-1})$ is embedded in the vertex v'_i by using Equation (13).

$$v''_i = v'_i + \varphi \vec{b}_{s_w}, \quad (13)$$

where v''_i is the modified vertex coordinate of v'_i , parameter φ is the embedding key, and $\vec{b}_{s_w} = (b_{s_w,x}, b_{s_w,y}, b_{s_w,z})$ is the corresponding direction vector of s_w .

Referring to Equation (13), data embedding in the encrypted domain is performed as

$$\begin{cases} \hat{c}_{i,j} = c_{i,j} \cdot c_{s_w} = E[v_{i,j}, r_{i,j}] \cdot E[-\varphi \cdot b_{s_w,j}, r_{s_w}]^{-1} \bmod N^2, & \text{if } \varphi \cdot b_{s_w,j} < 0, j \in \{1, 2, 3\}, \\ \hat{c}_{i,j} = c_{i,j} \cdot c_{s_w} = E[v_{i,j}, r_{i,j}] \cdot E[\varphi \cdot b_{s_w,j}, r_{s_w}] \bmod N^2, & \text{if } \varphi \cdot b_{s_w,j} > 0, j \in \{1, 2, 3\}, \\ \hat{c}_{i,j} = c_{i,j}, & \text{if } \varphi \cdot b_{s_w,j} = 0, j \in \{1, 2, 3\}, \end{cases} \quad (14)$$

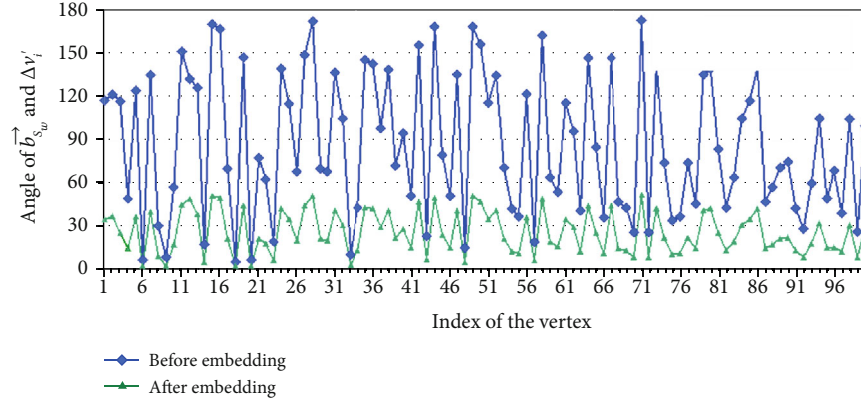


FIGURE 6: The changes of angle between prediction error $\Delta v'_i$ and direction vector \vec{b}_{s_w} before and after data embedding.

where $c'_{i,j}$ is the ciphertext of $v''_{i,j}$, and c_{s_w} is the ciphertext of $\varphi \cdot b_{s_w,j}$. Moreover, if $\varphi \cdot b_{s_w,j} > 0$, addition homomorphism of Paillier cryptosystem is utilized to embed secret data. If $\varphi \cdot b_{s_w,j} < 0$, subtraction homomorphism expansion of Paillier cryptosystem is utilized to embed secret data.

After data embedding, the corresponding change of the prediction error in the plaintext is as follows.

$$\Delta v'_i = \Delta v_i + \varphi \cdot \vec{b}_{s_w}. \quad (15)$$

After Δv_i being changed, the angle between the direction of prediction error and direction vector will be small.

In order to improve accuracy of data extraction, two inferences about vector are provided to calculate the embedded key.

Inference 1. Suppose that \vec{m}_1 and \vec{m}_2 are two three-dimensional vectors. If the directions of \vec{m}_1 and \vec{m}_2 are the same, the modulus length $|\vec{m}_1 + \vec{m}_2|$ has the maximum. If the directions of \vec{m}_1 and \vec{m}_2 are the opposite, the modulus length $|\vec{m}_1 + \vec{m}_2|$ has the minimum. The proof is listed as follows.

$$|\vec{m}_1 + \vec{m}_2|^2 = |\vec{m}_1|^2 + |\vec{m}_2|^2 + 2|\vec{m}_1| \cdot |\vec{m}_2| \cdot \cos \theta(\vec{m}_1, \vec{m}_2), \quad (16)$$

where $\theta(\vec{m}_1, \vec{m}_2)$ is the angle between \vec{m}_1 and \vec{m}_2 . According to Equation (16), since $|\vec{m}_1 + \vec{m}_2|$ is related to the angle, the above inference holds.

Inference 2. For two unit vectors \vec{n}_1 and \vec{n}_2 , let $\theta(\vec{n}_1, \vec{n}_2)$ denote the angle between two vectors, and let $\theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2)$ denote the angle between \vec{n}_1 and $\vec{n}_1 - \vec{n}_2$. $\theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2)$ and $\theta(\vec{n}_1, \vec{n}_2)$ are positively related. The smaller $\theta(\vec{n}_1, \vec{n}_2)$, the smaller $\theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2)$. In addition, $\theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2) \in [0, \pi/2]$. The proof is listed as follows.

$$\begin{aligned} \cos \theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2) &= \frac{\vec{n}_1 \times (\vec{n}_1 - \vec{n}_2)}{|\vec{n}_1| \cdot |\vec{n}_1 - \vec{n}_2|} \\ &= \frac{|\vec{n}_1|^2 - |\vec{n}_1| \cdot |\vec{n}_2| \cos \theta(\vec{n}_1, \vec{n}_2)}{|\vec{n}_1| \cdot |\vec{n}_1 - \vec{n}_2|}, \end{aligned} \quad (17)$$

where \times denotes cross product. Since \vec{n}_1 and \vec{n}_2 are unit vector, Equation (18) can be obtained according to Equation (17).

$$\cos \theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2) = \sqrt{(1 - \cos \theta(\vec{n}_1, \vec{n}_2))} / 2. \quad (18)$$

According to Equation (18), $\cos \theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2) > 0$, and $\theta(\vec{n}_1, \vec{n}_1 - \vec{n}_2) \in [0, \pi/2]$. The above inference holds.

3.3.5. Embedding Key Calculation. The embedding key influences the accuracy of data extraction. If the embedding key satisfies a certain condition, secret data can be extracted correctly.

Figure 5 shows the angle between prediction error and three direction vectors. Suppose that θ_{s_w} denotes the angle between prediction error Δv_i and direction vector \vec{b}_{s_w} corresponding to the secret data s_w , and θ_k denotes the angle between prediction error Δv_i and other direction vector \vec{b}_k ($k \in [0, 2^n - 1], k \neq s_w$). θ_{s_w} is computed as

$$\cos \theta_{s_w} = \frac{\Delta v'_i \times \vec{b}_{s_w}}{|\Delta v'_i| |\vec{b}_{s_w}|}. \quad (19)$$

Since the secret data is extracted by using the smallest angle between the prediction error and the direction vector, in order to improve the accuracy of data extraction, θ_{s_w} should be smaller than θ_k ($k \in [0, 2^n - 1], k \neq s_w$). After data embedding, Equation (20) should be satisfied.

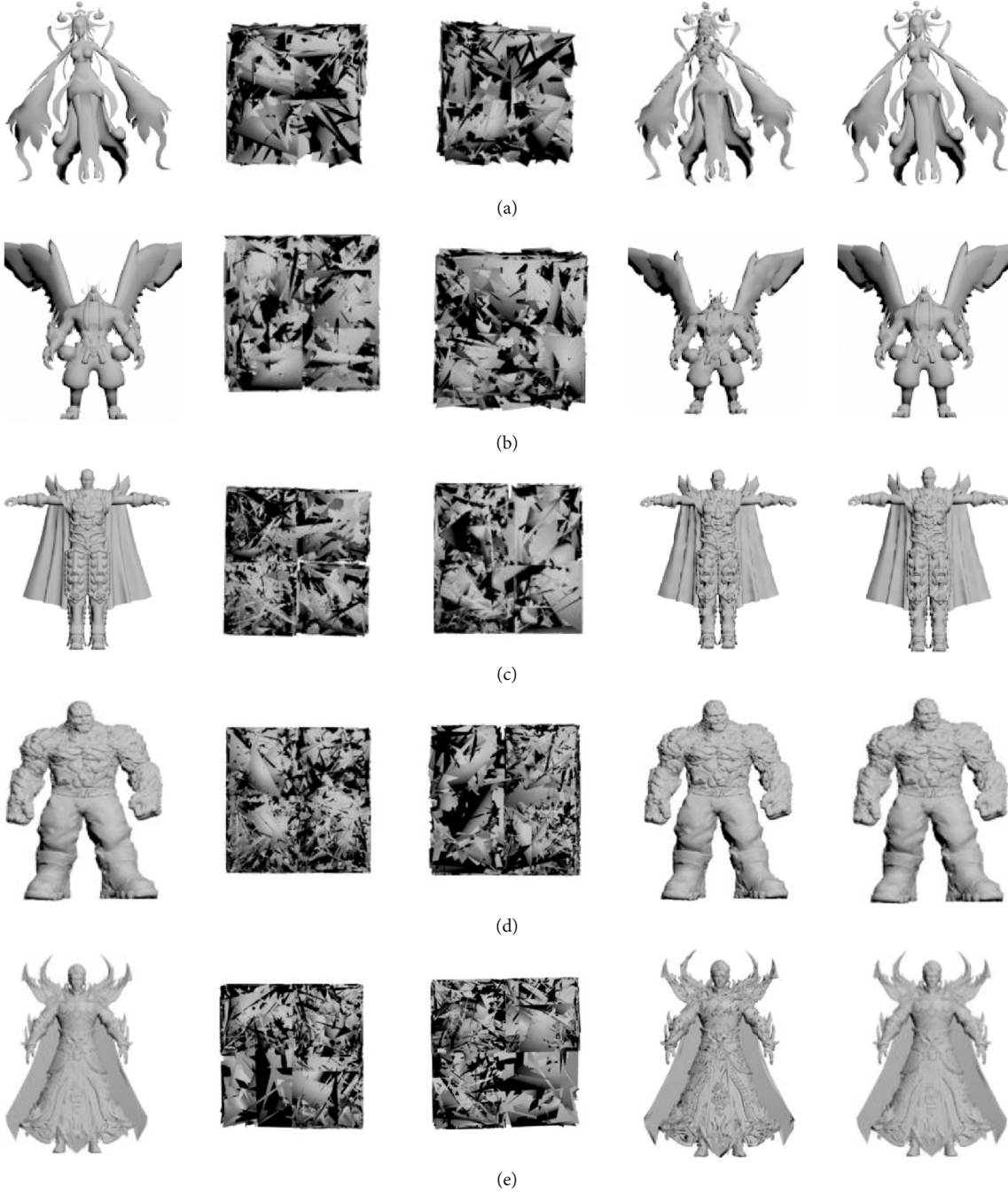


FIGURE 7: Illustrative examples showing the appearance of five models in different phases, include original 3D model, encrypted 3D model, data-embedded 3D model, directly decrypted 3D model, and recovery 3D model. (a) Fairy, (b) boss, (c) Devil, (d) Thing, and (e) Lord.

$$\forall k \in [0, 2^n - 1], k \neq s_w, \quad \cos \theta_{s_w} > \cos \theta_k. \quad (20)$$

It can be derived to the following equation.

The following equation can be derived by using Cosine Theorem.

$$\left(\Delta v_i + \varphi \vec{b}_{s_w} \right) \times \left(\frac{\vec{b}_{s_w}}{|\vec{b}_{s_w}|} - \frac{\vec{b}_k}{|\vec{b}_k|} \right) > 0. \quad (22)$$

$$\forall k \in [0, 2^n - 1], k \neq s_w, \quad \frac{\Delta v_i' \times \vec{b}_{s_w}}{|\Delta v_i'| |\vec{b}_{s_w}|} > \frac{\Delta v_i' \times \vec{b}_k}{|\Delta v_i'| |\vec{b}_k|}. \quad (21)$$

Suppose that the vector $\vec{M} = (\vec{b}_{s_w}/|\vec{b}_{s_w}| - \vec{b}_k/|\vec{b}_k|)$, and Equation (22) can be simplified as

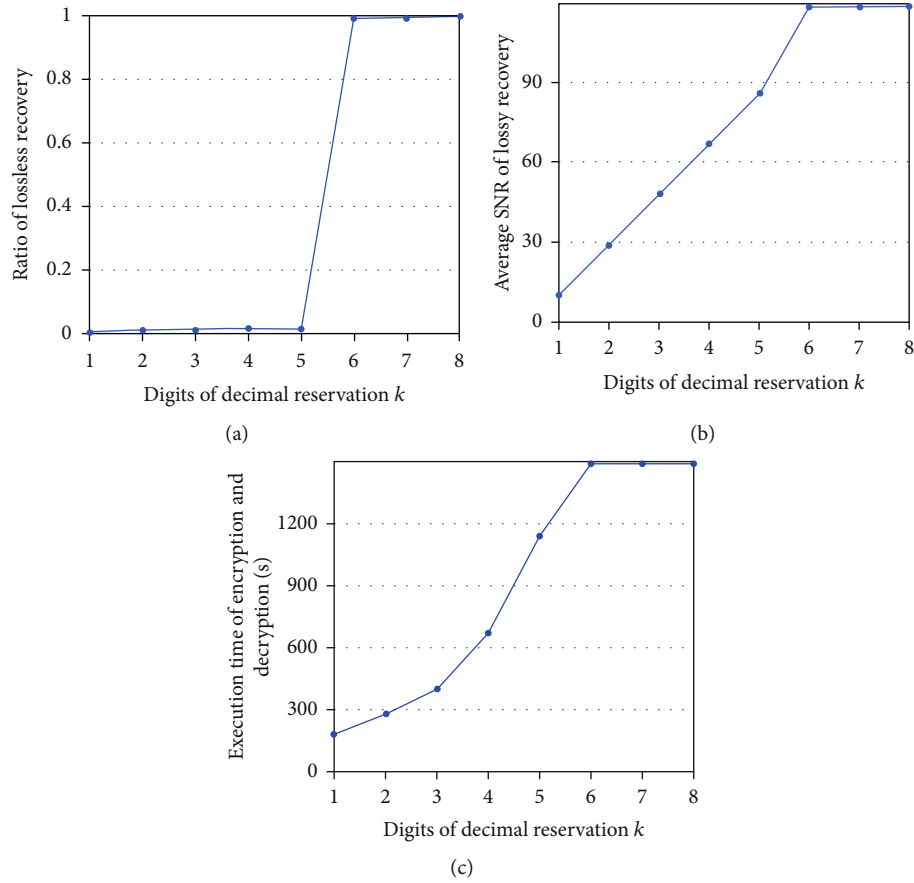


FIGURE 8: (a) Ratio of lossless recovery under different k . (b) Average SNR of decrypted model under different k . (c) Average execution time of encryption and decryption under different k .

$$\left(\Delta v_i + \varphi \vec{b}_{s_w}\right) \times \vec{M} > 0. \quad (23)$$

According to Inference 2, the angle between \vec{b}_{s_w} and \vec{M} is smaller than $\pi/2$, so $\vec{b}_{s_w} \times \vec{M} > 0$. Equation (24) can be derived.

$$\varphi > \frac{\Delta v \times (-\vec{M})}{\vec{b}_{s_w} \times \vec{M}}. \quad (24)$$

Since the modulus length $|\Delta v| \in [0, D]$, Equation (25) can be derived according to Inference 1.

$$\Delta v = \frac{D}{|\vec{M}|} \cdot (-\vec{M}), \quad \varphi > \left(\frac{\Delta v \times (-\vec{M})}{\vec{b}_{s_w} \times \vec{M}} \right)_{\max} = \frac{D \cdot |\vec{M}|}{\vec{b}_{s_w} \times \vec{M}}. \quad (25)$$

It can be derived to the following equation by using Cosine Theorem.

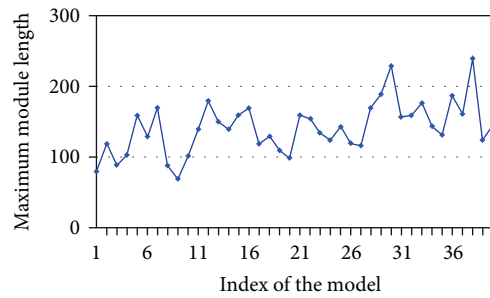


FIGURE 9: The maximum modulus length of forty 3D models.

$$\varphi > \frac{D \cdot |\vec{M}|}{|\vec{b}_{s_w}| \cdot |\vec{M}| \cdot \cos \theta(\vec{b}_{s_w}, \vec{M})} \Leftrightarrow \varphi > \frac{D}{|\vec{b}_{s_w}| \cdot \cos \theta(\vec{b}_{s_w}, \vec{M})}. \quad (26)$$

Suppose that $\theta(\vec{b}_{s_w}, \vec{M})$ denotes the angle between \vec{M} and \vec{b}_{s_w} , in order to ensure that θ_{s_w} is smaller than θ_k , θ_{s_w} should satisfy the following equation.

$$\varphi = \left[\frac{D}{\left| \vec{b}_{s_w} \right| \cdot \cos \theta \left(\vec{b}_{s_w}, \vec{M} \right)} \right]. \quad (27)$$

If φ satisfies Equation (27), secret data can be extracted correctly. According to Inference 2 and Equation (27), φ has the maximum if the angle between \vec{b}_{s_w} and \vec{b}_k is smallest.

Since direction vector is related to the shared parameters n , the shared parameters influence the value of φ . According to Equation (27), the relationship between φ and n is obtained as follows.

$$\begin{cases} \varphi = D, & \text{if } n = 1, 2, 3, \\ \varphi = \left\lceil \sqrt{3}D \right\rceil, & \text{if } n = 4, \end{cases} \quad (28)$$

For example, for a clear description, let $n = 3$. In this condition, the angle between $\vec{b}_0 = (-1, -1, -1)$ and direction vector $\vec{b}_1 = (-1, -1, 1)$ is the smallest. The embedding key can be calculated by the following equation.

$$\begin{aligned} \vec{M} &= \left(\frac{\vec{b}_0}{\left| \vec{b}_0 \right|} - \frac{\vec{b}_1}{\left| \vec{b}_1 \right|} \right) = \frac{1}{\sqrt{3}}(-1, -1, 2), \quad \cos \left(\vec{b}_0, \vec{M} \right) \\ &= \frac{1}{\sqrt{3}}, \varphi = \left[\frac{D}{\left| \vec{b}_0 \right| \cos \left(\vec{b}_0, \vec{M} \right)} \right] = D. \end{aligned} \quad (29)$$

In order to explain the whole processes, the data embedding example is given as follows. For convenience, suppose that $n = 2$, the i th vertex $v'_i = (1410, 2120, 790)$, the prediction value $\bar{v}_i = (1430, 2280, 750)$, and the secret data $w' = (1, 0)$. Since $n = 2$, the weighted sum $s_w \in [0, 3]$ according to Equation (11), and four direction vectors can be obtained according to the mapping table. Four direction vectors $\vec{b}_0 = (-1, -1, -1)$, $\vec{b}_1 = (-1, -1, 1)$, $\vec{b}_2 = (-1, 1, -1)$, and $\vec{b}_3 = (-1, 1, 1)$ correspond to $s_w = 0$, $s_w = 1$, $s_w = 2$, and $s_w = 3$, respectively. Since $w' = (1, 0)$, then $s_{w'} = 2$ can be computed, and $s_{w'} = 2$ corresponds to $\vec{b}_2 = (-1, 1, -1)$. In addition, $\varphi = 250$ can be obtained by Equation (28). The prediction error can be computed, and $\Delta v_i = (-20, -160, 40)$ according to Equation (9). Initially, the angle between Δv_i and $\vec{b}_0, \vec{b}_1, \vec{b}_2, \vec{b}_3$ can be computed, and $\theta_0 = 60.88^\circ$, $\theta_1 = 40.12^\circ$, $\theta_2 = 128.7^\circ$, and $\theta_3 = 110.3^\circ$. After data hiding, θ_2 between Δv_i and \vec{b}_2 should be the smallest angle. During data hiding, $v''_i = v'_i + \varphi \vec{b}_2$ and $\Delta v''_i = \Delta v_i + \varphi \vec{b}_2$. Hence, $v''_i = (1160, 2370, 540)$ and $\Delta v''_i = (-270, 90, -210)$. Then, $\theta_0 = 50.49^\circ$, $\theta_1 = 91.87^\circ$, $\theta_2 = 21.58^\circ$, and $\theta_3 = 75.83^\circ$ can be computed. The result shows

TABLE 3: The effect of the embedding key and shared parameter on bit error rate of data extraction.

n	φ					
	1	2	3	4	5	6
50	14.2%	17.3%	24.8%	33.5%	46.4%	46.7%
70	7.34%	9.12%	12.6%	23.4%	38.9%	38.9%
90	3.21%	4.25%	5.79%	16.5%	32.9%	32.9%
110	1.54%	2.25%	2.76%	10.8%	25.4%	25.5%
130	0.79%	1.22%	1.63%	6.86%	18.2%	18.3%
150	0.32%	0.63%	0.98%	4.25%	13.2%	13.3%
170	0.14%	0.26%	0.53%	2.84%	9.47%	9.47%
190	0.08%	0.11%	0.24%	1.77%	6.24%	6.25%
210	0.03%	0.05%	0.09%	1.25%	4.83%	4.83%
230	0.01%	0.02%	0.04%	0.84%	3.05%	3.06%
250	0	0	0	0.53%	2.24%	2.25%
270	0	0	0	0.32%	1.76%	1.76%
290	0	0	0	0.21%	1.43%	1.46%
210	0	0	0	0.15%	1.09%	1.09%
330	0	0	0	0.09%	0.79%	0.79%
350	0	0	0	0.04%	0.42%	0.42%

that θ_2 between $\Delta v''_i$ and \vec{b}_2 will be smallest after data hiding, and the secret data can be extracted by finding the smallest angle.

Figure 6 shows the changes of angles θ_{s_w} between prediction error $\Delta v''_i$ of 100 vertices and direction vector \vec{b}_{s_w} corresponding to secret data s_w before and after data embedding when the shared parameter is 3. The result shows that the angle will become smaller after data embedding.

In addition, a large embedding key will make 3D model disturbed obviously. Hence, the embedding key will be discussed specifically in Section 4 to balance the distortion of the directly decrypted model and the accuracy of data extraction.

3.4. Data Extraction and Model Recovery. After receiving the encrypted model with secret data, receiver can decrypt 3D model with private key λ and obtain the directly decrypted 3D model. The decryption of 3D model is as follows.

$$v''_{i,j} = D \left[c'_{i,j} \right] = \frac{L \left(\left(c'_{i,j} \right)^\lambda \bmod N^2 \right)}{L \left(g^\lambda \bmod N^2 \right)} \bmod N. \quad (30)$$

The directly decrypted 3D model is similar to the original model because only the coordinates of some vertices are modified slightly during data embedding.

After decrypting 3D model, all vertices are first classified into the embedded set and the referenced set using the dyeing algorithm. Secondly, prediction error of the vertex in embedded set is computed and the mapping table is constructed with the shared parameter n . Then, the angles between prediction error and all direction vector are computed, and the smallest angle θ_{s_w} is selected, which is the angle between

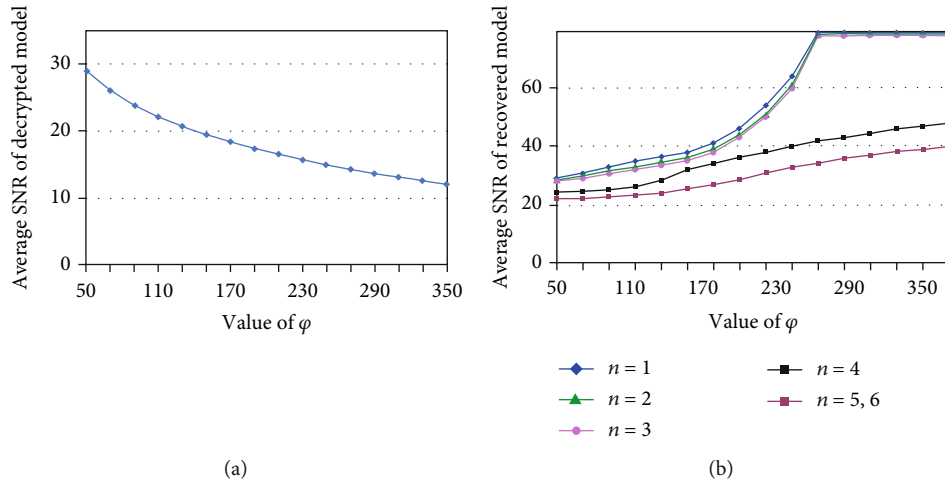


FIGURE 10: (a) The effect of the embedding key and shared parameter on SNR_D of decrypted model. (b) The effect of the embedding key and shared parameter on SNR_R of decrypted model.

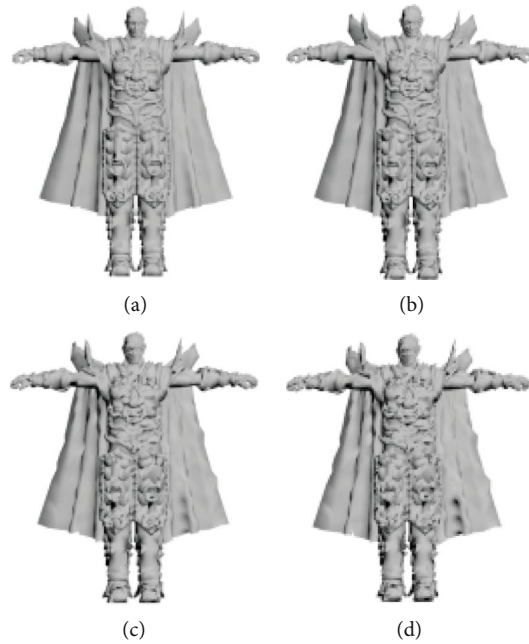


FIGURE 11: Four decrypted models devil when $n = 3$, and ϕ changes from 90 to 150. (a) $\phi = 90$, (b) $\phi = 110$, (c) $\phi = 130$, and (d) $\phi = 150$.

$\Delta v'_i$ and \vec{b}_{s_w} . At last, \vec{b}_{s_w} can be obtained, and the corresponding s_w can be found by using the mapping table.

s_w is converted into n bit $w(w_0, w_1, \dots, w_{n-1})$ by using

$$w_i = \left\lfloor \frac{s'_i}{2^i} \right\rfloor \bmod 2, \quad i = 0, 1, 2, \dots, n - 1. \quad (31)$$

After data extraction, the embedding key and direction vector can be used to recovery the original 3D model by using

$$v'_i = v''_i - \phi \cdot \vec{b}_{s_w}. \quad (32)$$

4. Experiment Results and Discussion

The proposed method was implemented in Matlab 2016b under Window 7. We implemented the following experiment on 100 3D models and calculated the average of 100 3D models. Figure 7 shows a group of experiment results of five 3D models in different parses. The phases from left to right are original 3D model, encrypted 3D model, data-embedded 3D model, directly decrypted 3D model, and recovered 3D model. Directly decrypted 3D models have low distortion, and recovered 3D models have high similarity compared to original 3D model.

The similarity of disturbed 3D models is evaluated by the signal-to-noise ratio (SNR). The higher the SNR, the better the imperceptibility after embedding watermark. SNR is computed as

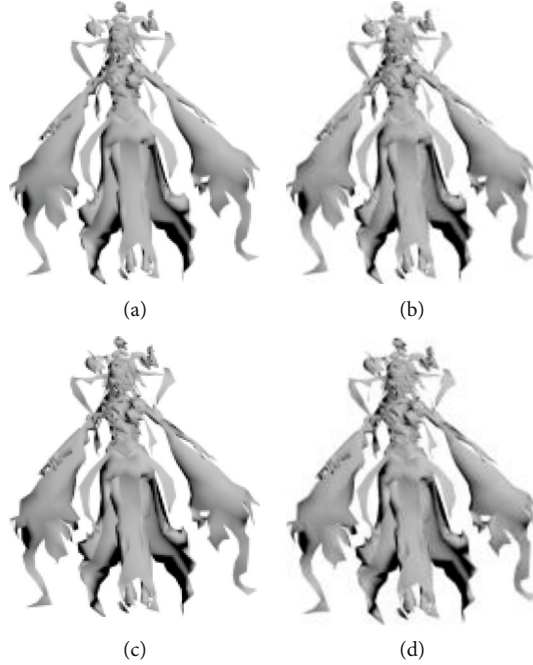


FIGURE 12: Four decrypted models fairy when n changes from 1 to 4. (a) $n = 1$, $\varphi = 110$; (b) $n = 2$, $\varphi = 110$; (c) $n = 3$, $\varphi = 110$; and (d) $n = 4$, $\varphi = 170$.

TABLE 4: The relationship between the number of the vertices and SNR_R .

Model	Vertices	D	Embedding rate	Error rate	SNR_D	SNR_R
Fairy	4252	205	83.7%	2.79%	18.43	34.79
Boss	10663	184	75.9%	2.54%	19.85	34.52
Devil	27872	169	77.8%	2.36%	21.32	35.16
Thing	110812	137	76.8%	2.88%	22.87	35.84
Lord	250343	118	77.4%	1.94%	24.16	35.32

$$\text{SNR} = 10 \lg \frac{\sum_{i=1}^{N_V} \left[(v_{i,x} - \bar{v}_x)^2 + (v_{i,y} - \bar{v}_y)^2 + (v_{i,z} - \bar{v}_z)^2 \right]}{\sum_{i=1}^{N_V} \left[(g_{i,x} - v_{i,x})^2 + (g_{i,y} - v_{i,y})^2 + (g_{i,z} - v_{i,z})^2 \right]}, \quad (33)$$

where $\bar{v}_x, \bar{v}_y, \bar{v}_z$ are the mean of vertex coordinates, $v_i(v_{i,x}, v_{i,y}, v_{i,z})$ are the original vertex coordinates, and $g_i(g_{i,x}, g_{i,y}, g_{i,z})$ are the coordinates of disturbed 3D model.

SNR_D is used to evaluate the similarity of directly decrypted models, and SNR_R is used to evaluate the similarity of recovered models. In addition, the bit error rate (BER) is used to measure the error rate of data extraction. The lower the BER, the higher the accuracy of data extraction.

4.1. Decimal Reservation Digits k . In order to observe the effect of decimal reservation digits k on the quality of the decrypted model and time cost, we changed the value of k from 1 to 8 and perform encrypting and decrypting on 3D models. As shown in Figure 8(a), $k = 6$ is a threshold, which enables 3D models recovery losslessly or limits recovery

losslessly. Since the significant digits of vertex coordinates is 6, it is easy to cause permanent distortion if $k < 6$. The distortion of directly decrypted model (SNR_D) is calculated, which is shown in Figure 8(b). The time cost of encryption and decryption is related to the value k , which is shown in Figure 8(c). In order to obtain high quality of decrypted models and reduce the time cost, k is set to 4 in the next experiment.

4.2. The Maximum of the Modulus Length D . D is the maximum of the modulus length of the prediction error. Due to the spatial correlation of natural 3D model, the actual value and its prediction value of the vertex coordinates are relatively close. Hence, the modulus length of the prediction error always is small. In order to calculate the range of the prediction error, the experiment is performed on 40 3D models. Figure 9 shows the maximum modulus length of 40 3D models. For all 3D models, it can be observed that all maximum modulus lengths are less than 250. Hence, D is set to 250 in the next experiment.

4.3. The Choice of the Embedding Key and the Shared Parameter. According to Equation (13), the embedding key φ directly affects the distortion of decrypted model. If φ is large and satisfies Equation (27), secret data will be extracted correctly, but the quality of 3D models will be decreased obviously. If φ is small, the change of prediction error also will be small, and the accuracy of data extraction will reduce. However, there are several existing methods that can improve the accuracy of data extraction, such as ECC code and BCD code. Hence, in order to balance the accuracy of data extraction and the decrypted model, the experiment is carried out by select φ from 50 to 350 with the interval of 20.

TABLE 5: The performance of the proposed method compared with the existing method.

Methods	Embedding key	BER	SNR _D	SNR _R	Capacity (bpv)
The proposed method	$\varphi = 110$	2.76%	22.13	35.12	0.872
	$\varphi = 250$	0	15.24	∞	0.872
Method in [26]		4.22%	5.35	31.97	0.369
Method in [28]		0	30.08	∞	0.396

The larger the shared parameter, the greater the embedding capacity. However, the larger the shared parameter leads to that, more direction vectors are constructed, which affects the accuracy of data extraction. The experiment is carried out by selecting n from 1 to 6.

Table 3 shows the effect of the embedding key and shared parameter on BER of data extraction. Figure 10(a) shows the effect of the embedding key and shared parameter on SNR_R of decrypted model. Figure 10(b) shows the effect of the embedding key and shared parameter on SNR_D of decrypted model. With the change of n from 1 to 4, there are corresponding values of φ with high accuracy and low distortion. When $n = 1$ and $\varphi = 110$, BER = 1.54%, SNR_D = 22.13, and SNR_R = 37.63. When $n = 2$ and $\varphi = 110$, BER = 2.25%, SNR_D = 22.13, and SNR_R = 35.83. When $n = 3$ and $\varphi = 110$, BER = 2.76%, SNR_D = 22.13, and SNR_R = 35.12. When $n = 4$ and $\varphi = 170$, BER = 2.88%, SNR_D = 17.28, and SNR_R = 34.85. It is observed that the proposed method has high accuracy, high embedding capacity, and low distortion when $n = 3$ and $\varphi = 110$.

Figure 11 shows decrypted models when $n = 3$, and φ changes from 90 to 150. Figure 12 shows decrypted model when n changes from 1 to 4.

4.4. The Effect of the Number of the Vertices on SNR_R. Table 4 shows the relationship between the number of the vertices and SNR_R. If a 3D model has a large number of vertices, then the distance between the adjacent vertices will become small, which makes 3D model has a small D . In addition, D directly influence SNR_R because of the relationship between D and ϕ . Hence, if a 3D model has more vertices, then the value of SNR_R will be small, which means that the decrypted model has low distortion.

4.5. Performance Comparison. In order to show the performance of the proposed method, we compare the proposed method with the existing method in [26] and in [28], as shown in Table 5. Compared with method in [26], the proposed method has three times the capacity and lower distortion than method in [26]. Moreover, the proposed has a lower BER, which can be reduced to zero by making the embedding key satisfy Equation (27).

Compared to method in [28], the embedding capacity of the proposed method is smaller. However, since several bits can be mapped to a direction vector using the mapping table, the capacity can be improved by embedding several bits into a vertex. Hence, the proposed method has a higher embedding capacity.

In the proposed method, the distortion and the accuracy can be adjusted by using the embedding key. When the embedding key is 110, 3D models after data hiding has lower distortion. When the embedding key is 250, the BER of data extraction can be reduced to zero. In addition, the distortion will increase as the embedding key increases, the BER will decrease as the embedding key decreases.

5. Conclusion

The method is proposed to preserve privacy and protect copyright of 3D models. Moreover, the proposed method has very good potential for practical applications since the directly decrypted models have lower distortion than the original models. Original 3D model is preprocessed, and the vertex of 3D model is encrypted by using Paillier cryptosystem. In the cloud, the dyeing method is designed to classify all vertices into the embedded set and the referenced set. After that, secret data is embedded by expanding direction of prediction error with direction vector. The prediction error of the vertex in the embedded set is computed by using the referenced set, and the direction vector is obtained according to the mapping table. Secret data can be extracted by comparing the angle between the direction of prediction error and direction vector, and the original model can be restored using the referenced set. The proposed method is efficient to protect copyright of 3D models in the cloud when the cloud administrator does not know the content of the 3D models. Moreover, the proposed has higher capacity and lower distortion than the existing methods.

For the future work of RDH-ED method, we will investigate the following two possible research directions. (1) Extracting information from plaintext is expanded to extracting from plaintext and ciphertext. (2) Further improve the similarity between the directly decrypted model and the original model.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

Authors' Contributions

The conceptualization and funding acquisition are credited to Li Li. The methodology and writing-original draft are due to Shengxian Wang. The conceptualization and supervision are credited to Ting Luo. The writing-review and editing are credited to Ching-Chun Chang. English grammar is credited to Qili Zhou. Formal analysis and investigation are originated by Hui Li. All authors read and approved the final manuscript.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (No. 61370218 and No. 61971247), Public Welfare Technology and Industry Project of Zhejiang Provincial Science Technology Department (No. LGG19F0-20016), and Ningbo Natural Science Foundation (No. 2019A610100).

References

- [1] X. Gao, L. An, X. Li, and D. Tao, "Reversibility improved lossless data hiding," *Signal Processing*, vol. 89, no. 10, pp. 2053–2065, 2009.
- [2] W. Liang, J. Long, C. Li, and J. Xu, "A fast defogging image recognition algorithm based on bilateral hybrid filtering," *ACM Transactions on Multimedia Computing, Communications, and Applications*, 2020.
- [3] W. Liang, W. Huang, J. Long, and K. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6392–6401, 2020.
- [4] J. Chen, F. Peng, J. Li, and M. Long, "A lossless watermarking for 3D STL model based on entity rearrangement and bit mapping," *International Journal of Digital Crime and Forensics*, vol. 9, no. 2, pp. 25–37, 2017.
- [5] Y. H. Huang and Y. Y. Tsai, "A reversible data hiding scheme for 3D polygonal models based on histogram shifting with high embedding capacity," *3D Research*, vol. 6, no. 2, pp. 1–12, 2015.
- [6] I. C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Transaction on Image Processing*, vol. 23, no. 4, pp. 1779–1790, 2014.
- [7] X. Zhang and S. Wang, "Fragile watermarking with error-free restoration capability," *IEEE Transaction on Multimedia*, vol. 10, no. 8, pp. 1490–1499, 2008.
- [8] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 97–105, 2003.
- [9] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transaction on Circuits and Systems*, vol. 13, no. 8, pp. 890–896, 2003.
- [10] Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," *IEEE Transaction on Multimedia*, vol. 10, no. 8, pp. 1500–1512, 2008.
- [11] A. Poljicak, L. Mandic, and D. Agic, "Discrete Fourier transform-based watermarking method with an optimal implementation radius," *Journal of Electronic Imaging*, vol. 20, no. 3, 2011.
- [12] B. Chen, G. Coatrieux, G. Chen, X. Sun, J. L. Coatrieux, and H. Shu, "Full 4-D quaternion discrete Fourier transform based watermarking for color images," *Digital Signal Processing*, vol. 28, pp. 106–119, 2014.
- [13] B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 5010–5021, 2013.
- [14] X. W. Li and S. T. Kim, "Optical 3D watermark based digital image watermarking for telemedicine," *Optics and Lasers in Engineering*, vol. 51, no. 12, pp. 1310–1320, 2013.
- [15] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transaction on Circuits Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.
- [16] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129–1143, 2009.
- [17] C. Y. Lin and S. F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," *Proceeding of Electronic Imaging*, vol. 3971, pp. 140–151, 2000.
- [18] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transaction on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.
- [19] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.
- [20] X. Cao, L. Du, and X. Wei, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Transaction on Cybernetics*, vol. 46, no. 5, pp. 1132–1143, 2016.
- [21] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Transaction on Signal Processing*, vol. 52, no. 10, pp. 2992–3006, 2004.
- [22] W. Liu, W. Zeng, and L. Dong, "Efficient compression of encrypted grayscale images," *IEEE Transaction on Image Processing*, vol. 19, no. 4, pp. 1097–1102, 2010.
- [23] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.
- [24] H. T. Wu and Y. M. Cheung, "A reversible data hiding approach to mesh authentication," in *Proceedings of International Conference on Web Intelligence*, pp. 774–777, 2005.
- [25] C. Y. Jhou, J. S. Pan, and D. Chou, "Reversible data hiding base on histogram shift for 3D vertex," *International Conference on International Information Hiding and Multimedia Signal Process*, 2007, pp. 365–368, Kaohsiung, Taiwan, 2007.
- [26] R. Q. Jiang, W. M. Zhang, and N. H. Yu, "Reversible data hiding in encrypted three-dimensional mesh models," *IEEE Transaction on Multimedia*, vol. 20, no. 1, pp. 55–67, 2018.
- [27] M. Shah and W. M. Zhang, "Homomorphic encryption-based reversible data hiding for 3D mesh models," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8145–8157, 2018.
- [28] L. Li, S. X. Wang, S. Q. Zhang, and T. Luo, "Homomorphic encryption-based robust reversible watermarking for 3D model," *Symmetry*, vol. 12, no. 3, pp. 347–365, 2020.
- [29] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the International Conference on Advance in Cryptology-Eurocrypt*, pp. 233–238, 1999.
- [30] K. Donald, *The Art of Computer Programming*, Addison-Wesley, Massachusetts, USA, 3rd edition, 1997.

Research Article

Construction of a Security Vulnerability Identification System Based on Machine Learning

Kebin Shi,¹ Yonghui Dai² and Jing Xu³

¹Advisory Department, Shanghai Information Investment Consulting Co., Ltd., Shanghai 200081, China

²Management School, Shanghai University of International Business and Economics, Shanghai 201620, China

³School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai 200433, China

Correspondence should be addressed to Yonghui Dai; dyh822@163.com

Received 19 February 2020; Revised 8 July 2020; Accepted 20 July 2020; Published 6 August 2020

Academic Editor: Fei Yu

Copyright © 2020 Kebin Shi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, the frequent outbreak of information security incidents caused by information security vulnerabilities has brought huge losses to countries and enterprises. Therefore, the research related to information security vulnerability has attracted many scholars, especially the research on the identification of information security vulnerabilities. Although some organizations have established information description databases for information security vulnerabilities, the differences in their descriptions and understandings of vulnerabilities have increased the difficulty of information security precautions. This paper studies the construction of a security vulnerability identification system, summarizes the system requirements, and establishes a vulnerability text classifier based on machine learning. It introduces the word segmentation, feature extraction, classification, and verification processing of vulnerability description text. The contribution of this paper is mainly in two aspects: One is to standardize the unified description of vulnerability information, which lays a solid foundation for vulnerability analysis. The other is to explore the research methods of a vulnerability identification system for information security and establish a vulnerability text classifier based on machine learning, which can provide reference for the research of similar systems in the future.

1. Introduction

With the rapid development of the Internet, various applications and information systems based on the Internet bring convenience and efficiency to individuals and enterprises. At the same time, it also brings a lot of information security problems [1]. According to a report released by the National Computer Virus Emergency Response Center of China, a total of 7,478,639 viruses were found in December 2018, and the main transmission routes of the virus were a phishing website, Trojan virus, and information security vulnerabilities [2]. In essence, information security refers to the defects of software. Once these defects are found and used by attackers, it is very easy to cause information theft and leakage and system damage, which often leads to huge losses [3]. For example, spectre and meltdown hacks attack behavior caused by CPU chip vulnerability [4], which involves many smartphones, personal computers, and servers [5]. As an important guarantee for the stable operation of the system, information security covers a

wide range of security protocols, such as SSH, SSL, and set [6], and network security authentication mechanisms such as digital authentication, digital signature, digital time stamp, and computer security operating system [7]. Because the software itself inevitably has defects, it causes security vulnerabilities. How to detect and prevent security vulnerabilities has always been one of the research hotspots in the field of information security.

In recent years, countries all over the world pay more and more attention to security vulnerabilities. A large number of security vulnerabilities have been found, which makes vulnerability management face many problems to be solved, such as the judgment and processing of vulnerability redundant data. The direct manifestation is that although there are many vulnerabilities, these vulnerabilities have the same characteristics and should be classified as similar vulnerabilities. However, the lack of a unified vulnerability identification rule makes the above vulnerabilities exist in the vulnerability database and causes vulnerability redundancy. In addition, the

correlation analysis of vulnerability, description, and identification of vulnerabilities are important contents in vulnerability management, which is very important for the construction of information security.

The remaining parts of this article are organized as follows: In Section 2, literature review is introduced. In Section 3, the vulnerability classification and machine learning method are shown. In Section 4, the system framework and design are introduced. In Section 5, the key technologies of TextRank keyword extraction and attribute extraction based on frequency are shown. Section 6 is the conclusion and discussion of this article.

2. Literature Review

2.1. Vulnerability Library and Detection Technology. At present, some security service organizations around the world have established their own vulnerability libraries. Common network vulnerability libraries mainly include CVE (Common Vulnerabilities and Exposures), NVD (US National Vulnerability Database), and CNVD (China National Vulnerability Database) [8]. Among them, each CVE vulnerability has a unique name corresponding to the CVE dictionary, which helps users distinguish vulnerabilities from vulnerability databases and detection tools [9]. If the vulnerability in the information security monitoring report belongs to a vulnerability in the CVE database table, then the corresponding patch solution can be obtained through the vulnerability name to solve the information security problem in time. For example, a CVE vulnerability number is CVE-2008-1046. NVD refers to the United States National Vulnerability Database [10]; its description of vulnerabilities includes 15 attributes such as vulnerability number, release date, vulnerability description, hazard type, attack path, and vulnerability type. It is widely used in global information security vulnerability services. CNVD is China's national information security vulnerability sharing platform. As China's official vulnerability release and security early warning platform, it plays an important role in the basic service of China's information security. The number of vulnerabilities released by it is CNVD-2019-0282. In addition, some security protection companies in China have also invested in the construction of vulnerability information resource libraries, such as the sky mirror vulnerability information resource library, which is a resource library for the announcement and protection of computer security vulnerabilities established by the company. It collected a variety of vulnerabilities and protection tools to provide users with vulnerability detection, patching, and attack verification, which improved the level of forensics and verification [11].

From the perspective of time, information security vulnerabilities often show the characteristics of the time life cycle. It will go through the process of creating and dying out of vulnerabilities. In the above process, the vulnerability presents phase characteristics. For this reason, some scholars divide the characteristics of information security vulnerabilities according to time, such as 0-day vulnerability and 1-day vulnerability [12]. In the research of vulnerability technology, more representative technologies mainly include APT detec-

tion technology, big data-based network vulnerability scanning technology, clustered vulnerability analysis technology, and intelligent vulnerability mining technology. At present, network security vulnerability detection systems include both paid commercial systems and open-source free leak scan systems, such as 360 security guards in China, Norton, Avast, and IBM Rational AppScan. APT detection and defense are an important content of information security. Chinese scholars have conducted research on user behavior and network traffic and applied social engineering to propose a baseline-based APT detection, which has traced and confirmed the APT attack [13]. Some scholars have proposed a method for predicting intrusion detection events based on APT and the functional configuration of the method, and they implemented a prediction model based on intrusion detection events through testing at the stages of learning, prediction, and evaluation [14]. With the gradual increase in software types and the development of information technology, it will become a trend to conduct large-scale vulnerability detection based on big data, artificial intelligence, and machine learning technologies in the future.

2.2. Review of Machine Learning in Network Security. In recent years, with the development of big data and artificial intelligence technology, recognition based on machine learning has been widely used in data analysis. In essence, machine learning is to simulate human learning behavior through computers. Experience is used as input, through continuous learning and iteration to train and build learning behavior models, so as to meet human-like standards for identification and prediction [15]. The common algorithms of machine learning include a regression algorithm, association rule, support vector machine, clustering algorithm, decision tree algorithm, artificial neural network, and deep learning. Some scholars have analyzed and compared the application technologies of machine learning in software defect finding, malicious code detection, and intrusion detection, including linear discriminant analysis, decision tree analysis, multiple linear regression, rough set, support vector machine, and artificial neural network [16].

The application of a machine learning algorithm in network security includes security intrusion detection, spam detection, and domain name detection [17]. For example, through the use of a random forest algorithm and SVM support vector machine algorithm, the Chinese scholars take the KDD Cup 99 data set as the sample for intrusion detection simulation analysis and get the data of the above algorithm on the false alarm rate, training time, model memory occupation, and unknown attack detection ability, as well as the advantages and disadvantages of each algorithm [18]. Some scholars use Weka and RapidMiner to evaluate the performance of a machine learning algorithm for spam detection on Twitter [19]. Their research results provide a reference for antispam. For better monitoring, some scholars put forward the MLH-IDS machine learning framework, which consists of three layers: supervised learning layer, unsupervised learning layer, and outlier detection layer. The advantages of different machine learning methods are comprehensively described, so that the framework can show more flexibility

and good performance [20]. In addition, some scholars layered the data, combined the SVM support vector machine and the ELM algorithm, and built a multilayer hybrid intrusion detection model. The model was tested on the KDCUP99 data set and achieved an accuracy of 95.75% [21].

3. Theory and Technology

3.1. Vulnerability Classification. Vulnerability classification refers to the classification of vulnerabilities. From the perspective of mathematical thinking, the vulnerability classification process is a mapping process. It classifies vulnerabilities that need to be classified into existing vulnerability categories according to a certain mapping relationship. The vulnerability category refers to the type of vulnerability, which is divided into categories based on attributes such as the cause of the vulnerability, the scope of action, the technology used, and the location characteristics.

There are many forms of information security vulnerability and its deformation. Therefore, many countries have established a special information security vulnerability database. As an important force of information security maintenance in the century, China has established the China National Vulnerability Database of Information Security (CNNVD), which comprehensively describes the classification of vulnerabilities. It mainly includes general vulnerability, event vulnerability, and public vulnerability. Specifically, it divides vulnerabilities into 26 categories, including configuration errors, input verification, code problems, and SQL injection. A sample of vulnerability types is shown in Figure 1 [22].

It can be seen from Figure 1 that the first level of vulnerability is divided into three major categories, namely, configuration errors, code problems, and insufficient information. Among them, the code problem category can be divided into sublevel categories. In the above vulnerabilities, configuration error vulnerability refers to the vulnerability in the process of software configuration, which is caused by unreasonable configuration in the use of the software.

3.2. Machine Learning. Machine learning, literally, means to provide some data to personal computers, servers, and other machines and let them learn and find out the logic of data through mathematical modeling and self-iterative method, and then, it can automatically complete prediction, classification, and recognition once it faced similar data. At present, machine learning has been widely used in pattern recognition, visual visualization, and network intrusion detection and other fields [23]. From the perspective of the application of machine learning, it can be divided into five categories: supervised learning, semisupervised learning, unsupervised learning, transfer learning, and reinforcement learning [24]. The complete process of machine learning consists of business understanding, data collection, data preprocessing, data modeling, and model evaluation [25]. Among them, business understanding refers to understanding the needs and background knowledge of the task before performing the task of machine learning. The data collection mainly includes the collection and storage of the original data, which is the premise of follow-up work and provides the basis for future

work. Data preprocessing is to clean and transform the original data, which is a very important process in machine learning. In this process, effective information needs to be extracted as much as possible to prepare for subsequent modeling. Data modeling refers to the establishment of a data model by machine learning methods such as supervised learning, unsupervised learning, and reinforcement learning. The classic supervised learning algorithms include artificial neural networks, naive Bayes, and decision tree analysis, and the classical unsupervised learning algorithms include clustering and dimension reduction. Model evaluation refers to the use of some relevant methods and indicators to evaluate the advantages and disadvantages of the model obtained by a machine learning algorithm, and its common evaluation indexes include precision, recall, F -value, and accuracy.

SVM (support vector machine) is a typical algorithm in machine learning. Its core idea is to find the most suitable separation hypersurface in the sample space, which can distinguish the samples significantly. Common forms of SVM include linear separable, linear support, and nonlinear support vector machines. Among them, the linear regression of SVM is expressed as follows.

Set the sample set as $(y_1, x_1), \dots, (y_l, x_l), x \in R^n, y \in R$, and use a linear equation to represent the regression function.

$$f(x) = \omega^T \varphi(x) + b. \quad (1)$$

The essence of formula (1) can be regarded as a constrained optimization problem, and its expression is as follows.

$$\varphi(\omega, \xi, b) = \frac{1}{2} |\omega|^2 + C \left(\sum_{i=1}^l \xi_i + \sum_{i=1}^l \xi_i^* \right). \quad (2)$$

In formula (2), C refers to the penalty factor and ξ and ξ^* represent the upper and lower limits of the relaxation variable, respectively. Formula (2) is solved by the Lagrangian constraint equation, which is shown as follows.

$$\bar{\alpha}, \bar{\alpha}^* = \arg \min \left\{ \begin{array}{l} \frac{1}{2} \sum_{i=1}^l \sum_{j=1}^l (\alpha_i - \alpha_i^*) (\alpha_j - \alpha_j^*) (\varphi(x_i) \varphi(x_j)) \\ - \sum_i (\alpha_i - \alpha_i^*) y_i + \sum_i (\alpha_i + \alpha_i^*) \varepsilon \end{array} \right\}, \quad (3)$$

In formula (3), $\varphi(x)$ is a kernel function. If $\varphi(x_i) \varphi(x_j) = x_i x_j$, then it represents a linear support vector machine; otherwise, it is a nonlinear support vector machine. The solution expressions of the sum of the coefficients to be

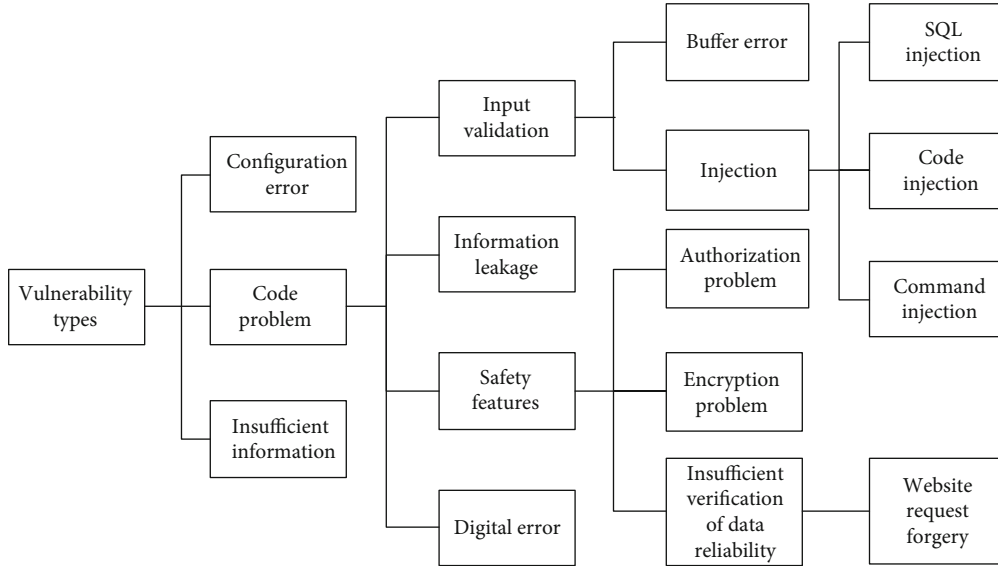


FIGURE 1: Sample of vulnerability types.

determined, the regression coefficients, and the constant terms are as follows.

$$\begin{aligned} \bar{\omega} &= \sum_{i=1}^l (\alpha_i - \alpha_i^*) x_i, \\ \bar{b} &= -\frac{1}{2} \bar{\omega} [x_r + x_s]. \end{aligned} \quad (4)$$

In a kernel function, the Gaussian kernel is widely used. It is also called radial basis kernel (RBF kernel), and its expression is as follows:

$$\varphi(x_i) \varphi(x_j) = \exp \left(-\frac{|x_i - x_j|^2}{2r^2} \right). \quad (5)$$

In formula (5), r refers to the variance of the Gaussian function in the Gaussian kernel function.

4. System Design

4.1. System Design Objectives. A security vulnerability identification system is an important part of information security construction. The design of the system based on machine learning is of great significance for timely and accurate determination of a vulnerability category and hazard level and provision of a complete data source for researchers. On the basis of full investigation, the principles of system objective design are as follows.

- (1) The system needs to follow the principles of flexibility and scalability. It should have good scalability and meet the needs of future upgrades
- (2) The system needs to follow the principle of adaptability, and it should have environmental adaptability

and consider the needs of users in order to adapt to various user operations

- (3) The system should have the function of authority grading. In the system, the access control rights of users with different permission levels are different, and it is necessary to strictly control the user's rights of adding, deleting, modifying, and searching
- (4) The system should follow the stability principle and consider the safety and stability of operation. It should have corresponding measures in antivirus attack, data backup, and data recovery
- (5) The system design should follow the principle of modularization and divide the function of the system reasonably. For example, it has the data preprocessing module, which is responsible for cleaning the dirty data and processing the distorted data or integrated data. It has the function of vulnerability rule management, which is responsible for the addition, deletion, modification, and query of rules. It has the function of vulnerability data identification and classification

4.2. System Requirement Analysis. The purpose of the security vulnerability identification system is to integrate and uniformly manage the data and information of various vulnerability databases. It can collect, summarize, and display vulnerability data. After investigation and analysis of the current situation, the requirements of the security vulnerability identification system are summarized as follows.

4.2.1. Requirements for Establishing a Unified Vulnerability Database Description. A vulnerability knowledge database is an important accumulation of current vulnerability knowledge in the field of network security. For different vulnerability databases, there may be the same vulnerability information,

but the rules of the vulnerability number are all customized, which increases the difficulty of vulnerability knowledge management. There are many security vulnerability databases domestically and internationally such as vulnerability databases of CVE, CNNVD, and CNVD. Different security vulnerability databases have different naming and numbering rules. For example, the typical numbering method of CVE vulnerability databases is “cve-2014-4664,” which is a vulnerability number. Therefore, the current main numbering rule is vulnerability database name plus discovery year plus vulnerability sequence number. Another example is a vulnerability identified as “cnvd-2017-17486” in the CNVD vulnerability database. This vulnerability belongs to buffer overflow vulnerability, which occurs in basic applications such as a database and causes database service interruption. The scope and harm of this vulnerability will be relatively wide. However, the vulnerability “cnvd-2017-17486” was found by a company in China. There is no corresponding vulnerability number in CVE. In order to better conduct vulnerability analysis, it is necessary to form a relatively unified vulnerability database.

4.2.2. Requirements for Data Quality. Because data analysis is based on a single data set, when there is data from multiple data sets, a unified preprocessing of the multiple data is required to improve the quality of the data so that the subsequent analysis can be better performed [28]. In order to improve the data quality, this paper establishes the identification management and rule-making. After the original data is obtained, the original data needs to be effectively sorted out according to the identification before it can be used for subsequent analysis. Usually, the first step is to standardize the data. Since the data processing is based on the identification data, the efficiency of data analysis and data tracing can be greatly improved.

At the same time, in order to improve the comprehensive utilization efficiency of all kinds of data, it is necessary to collect, process, and integrate the data of different data providers. In this paper, the open interface is used to manage the vulnerability rules, and the collected data is sorted into preprocessing data according to the specified format. The system takes identification rules as an important process of basic data processing and provides services for rule management, data analysis, and presentation of vulnerabilities, so as to realize centralized control and analysis of various data, especially to control data duplication and distortion and improve data quality.

4.3. System Framework. According to the requirements of the system, the system is divided into four layers: business presentation layer, application system layer, application support layer, and data resource layer. The system framework is shown in Figure 2.

The business presentation layer displays the business functions of each application management module according to the position and authority of the login personnel, such as the authority of adding, deleting, modifying, and querying the rule management function module.

The application system layer mainly relies on the various services provided by the application support layer and pro-

vides users with application software modules of the vulnerability security system according to the actual needs, including rule management, task management, data processing, result query, and data display functions.

The application support layer completes the interface services and management services related to system functions, including unified data interface, message middleware, distributed storage management, and security log audit, as well as various basic information online query and comprehensive query services and comprehensive analysis services.

The data resource layer encapsulates the data-related content, including text file, Excel file, XML file, and JSON file.

5. Key Technologies

5.1. TextRank Keyword Extraction. In the research of text classification, the support vector machine algorithm has good generalization ability, and it has a significant effect on small sample nonlinear classification. Therefore, this paper uses a support vector machine to achieve text classification. The process of text classification is complicated, mainly including text preprocessing, feature selection, classifier selection, and performance evaluation, which is shown in Figure 3.

It can be seen from Figure 3 that the process of classifying vulnerability description is as follows: firstly, text preprocessing is carried out for training data, including text segmentation, and a text model is used for characterization after removing stop words with little classification significance such as punctuation marks and characteristic characters; then, feature selection is carried out for the text model and features matching weight are selected, and then, a classification model is constructed and use the test data set to evaluate the performance of the classification model. If it meets the requirements, the classifier is selected for text classification. For example, the following vulnerability description information is classified and implemented as shown in Figure 4.

After the segmentation, the interjections, auxiliary verbs, and conjunctions are removed, and then, the characteristic words such as “SQL, database, deception, server, and malice” are selected for model training and output. In SVM classification, the choice of penalty parameter C and kernel parameter g is closely related to the performance of the SVM classifier. They control the empirical risk and VC confidence, respectively. In this study, the penalty parameter $C = 80.1532$ and kernel parameter $g = 0.23$ are obtained by continuous optimization of the kernel function.

TextRank’s idea of keyword extraction is based on PageRank’s idea. PageRank, as its name implies, ranks the importance of web pages. Its core idea has two main points. One is that if a web page has a large number of links with other web pages, it means that the importance of this web page is relatively high, and its PageRank value is relatively large; the other is that if a web page with a large PageRank value is compared with another page that has links, the PageRank value of the page connected with this large PageRank value will be increased accordingly. The advantage of PageRank is that the PageRank value of all its pages can be calculated statistically offline, but it also has the disadvantage that the old PageRank value is higher than the new one.

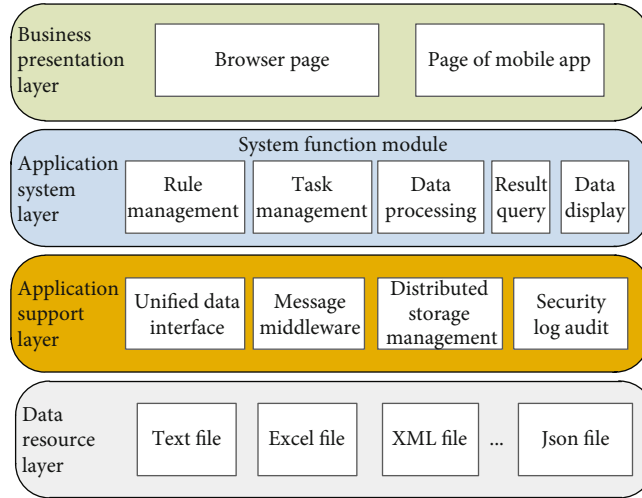


FIGURE 2: The system framework.

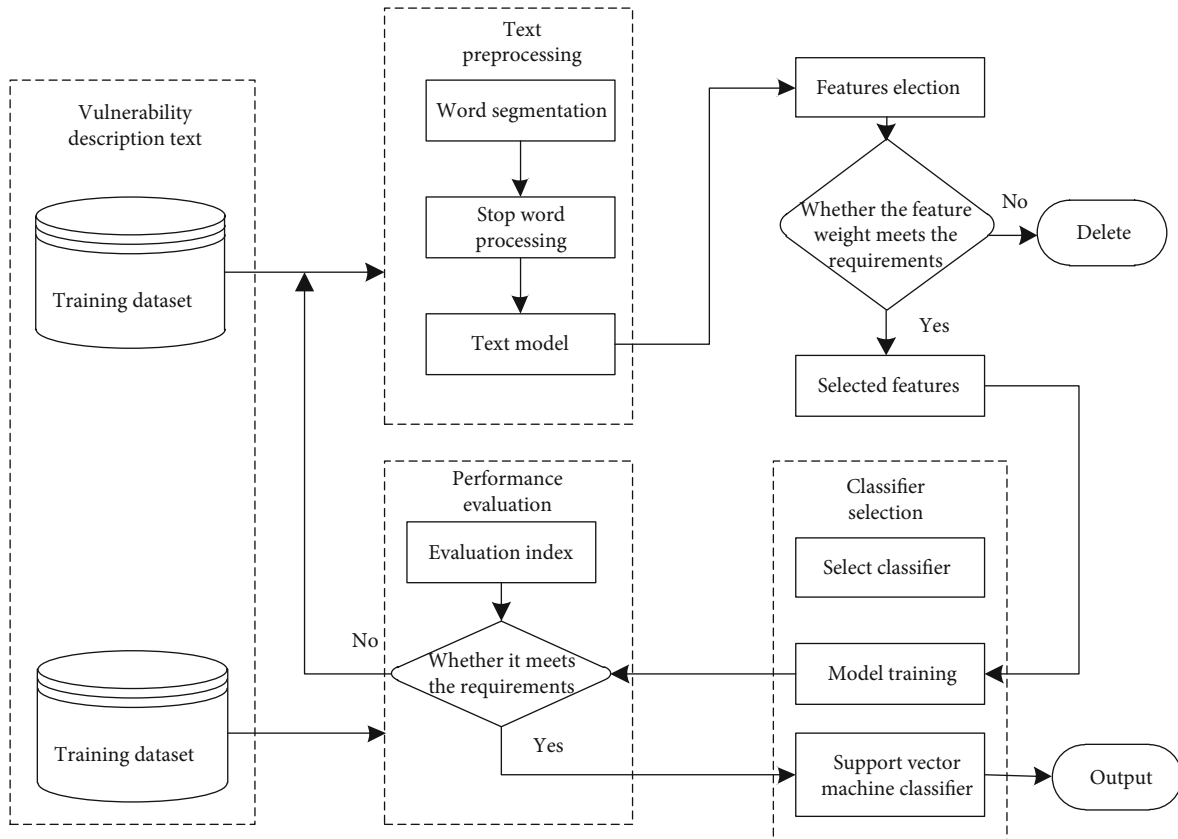


FIGURE 3: The process of text classification.

Because the keywords of text are similar to those of web pages, PageRank can be used to extract the keywords of text by modifying it to TextRank. The calculation of the TextRank value is as follows.

$$V(W_k) = (1 - d) + d * \sum_{W_j \in I(W_k)} \frac{\text{link}(W_k, W_j)}{\sum_{W_i \in O(W_j)} \text{link}(W_i, W_j)} V(W_j). \quad (6)$$

In formula (6), $V(W_k)$ is the importance value of keywords, $\text{link}(W_k, W_j)$ is the connection between words, $I(W_k)$ is the word set of word W_k , $O(W_j)$ is the word set of word W_j , and the damping factor D is 0.85. For example, the description of CNNVD information security vulnerability no. is cnnvd-201905-408. "There is a vulnerability in Microsoft Windows with security features. The vulnerability is due to the lack of authentication, access control, rights management, and other security measures in the network

漏洞描述:
 当应用程序使用输入内容来构造动态SQL语句以访问数据库时, 如果对输入的参数没有进行严格的过滤或者过滤不完整将会导致SQL注入攻击的产生。恶意用户通过构造特殊的SQL查询语句把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串, 最终达到欺骗服务器执行恶意的SQL命令。从而可以获取到数据库的相关信息, 包括数据库账号密码信息, 甚至可上传木马, 从而控制服务器。

漏洞描述:

p vn n v v n v vn n n n c
 "当" "应用" "程序" "使用" "输入" "内容" "来" "构造" "动态" "SQL" "语句" "以"
 v n x c p v u n v v ad u
 "访问" "数据库" "时" "如果" "对" "输入" "的" "参数" "没有" "进行" "严格" "的"
 v c v d a d x v n v v u
 "过滤" "或者" "过滤" "不" "完整" "将" "会" "导致" "SQL" "注入" "攻击" "的"
 vn d n v n a u n v n p n
 "产生" "恶意" "用户" "通过" "构造" "特殊" "的" " " " "查询" "语句" "把" "SQL"
 n v v n n v c v n c n vn
 "命令" "插入" "到" "Web" "表单" "递交" "或" "输入" "域名" "或" "页面" "请求"
 u v n n d v v n v d u n
 "的" "查询" "字" "符串" "最终" "达到" "欺骗" "服务器" "执行" "恶意" "的" "SQL"
 n c v v v n u vn n v n
 "命令" "从而" "可以" "获取" "到" "数据库" "的" "相关" "信息" "包括" "数据库"
 n n n x c v n c v n
 "账号" "密码" "信息" "甚至" "可" "上传" "木马" "从而" "控制" "服务器"

FIGURE 4: Examples of text segmentation.

system or product.” After word segmentation, we get “Microsoft Windows / presence / security / feature / problem / vulnerability / network system / lack / authentication / access / control / authority / management / security measures.” Then, we extract keywords and filter them according to the part of speech. The sliding window span is 5 and 7. The evaluation results are shown in Table 1.

In Table 1, precision refers to the actual positive data among all predicted positive data, which describes whether the prediction is accurate. Recall rate refers to the probability that all the real positive data are detected as positive examples, which represents the degree of integrity of all positive data. F1-measure combines the above two indexes of precision and recall, which represents the performance of classification. If the F1-measure value is higher, the performance of the classifier will be better.

5.2. Attribute Extraction Based on Frequency. Frequency-based attribute extraction is to identify and extract entity attribute information by making statistics of word frequency in vulnerability description text. Firstly, the middle noun of the comment sentence is identified by a POS tagger. The starting point of this idea is that the words with high frequency are important attribute words. Therefore, low-frequency words are usually not regarded as important words, and frequently occurring phrases are often important naming entities in this field.

The basic assumption of this method is that there are many text description information of vulnerability, and it is aimed at the same vulnerability, such as SQL injection. For example, a mutual information (PMI) score was used to calculate candidate phrases and entity classes with a “part whole

relationship,” in which the calculation formula of PMI is as follows.

$$PMI(x, y) = \frac{h(a \cap d)}{h(a)h(d)}, \quad (7)$$

In the above formula, a is the candidate attribute word identified by the word frequency statistical method, D is the indicator word, and the search engine calculates the frequency information of word occurrence and cooccurrence. When the PMI value is too small, it means that a and D will not coexist frequently, which may not be a component.

For example, for CNNVD (China National Information Security Vulnerability Database) information security vulnerability description numbered cnnvd-201903-843, the word frequency is extracted. The extraction results of the first 16 words are shown in Table 2. The weight in the table is calculated based on the vulnerability description information and the existing records in the database.

Network management includes two aspects: network equipment management and network performance management. Network equipment management requires remote management and maintenance through the monitoring and parameter adjustment of the primary operation of the equipment to ensure the availability and safety of the network; network performance management ensures the reliability and efficiency of the network and optimizes the quality of the network through the monitoring and adjustment of various performance indicators. In order to achieve a unified and efficient management, it is necessary to conduct a comprehensive analysis of the problems in the whole system and analyze the network events together with the system,

TABLE 1: Assessment results.

Value of sliding window	Precision	Recall	F1-measure
Span = 5	0.7341	0.7173	0.7524
Span = 7	0.7412	0.7231	0.7572

TABLE 2: Word frequency analysis.

No.	Keywords	Word frequency	Normalized weight
1	Postscript	3	1
2	Artifex	3	1
3	Software	3	1
4	Ghostscript	2	0.9354
5	PostScript	2	0.9354
6	Loophole	2	0.8874
7	Open source	1	0.8471
8	United States	1	0.8314
9	Desktop	1	0.8302
10	Program	1	0.825
11	Attacker	1	0.824
12	Safety	1	0.8239
13	Parsing	1	0.8239
14	Table of contents	1	0.8231
15	Access	1	0.8201
16	Page	1	0.8181

database, and application events, so as to analyze the root causes of the problems. It can easily manage the switching network through the graphical interface, including remote monitoring, management and configuration of equipment, division and configuration of VLAN, and monitoring of network traffic.

6. Conclusion and Discussion

Firstly, this paper introduces the research status of information security vulnerability and machine learning identification domestically and internationally, including NVD in the United States, CNVD of the national information security vulnerability sharing platform in China, and detection system of network security vulnerability and the application of machine learning in network security, and then expounds the related concepts and technologies of information security vulnerability identification, including vulnerability types, text classification, and machine learning algorithm. Then, it analyzes the requirements of a vulnerability identification system, including the identification model, system requirements, and functional requirements, and introduces the design of a security vulnerability identification system, including the overall framework design, functional module design, database design, error tolerant security design, and text classification design based on the above design; it gives the information security vulnerability. The system implementation of the identification system and the key technologies of vulnerability text classification are introduced.

With the continuous advancement of network informatization, information security vulnerability identification will face greater challenges. The article has carried out some exploration and research on the security vulnerability identification system. Future research work can be improved from the following aspects. (1) The description of vulnerability text features can be improved. Since vulnerability text feature description is the basis of information security vulnerability identification, whether its representation is universal and accurate is critical to the security vulnerability identification system. Therefore, in-depth research will be conducted in the future on the characteristics of the vulnerability text so as to be able to filter out more accurate text feature items and improve the recognition accuracy and efficiency. (2) The design and implementation of the classifier can be improved. Feature selection is a key content in the text classification process, and the quality of the selection often directly determines the final classification result. Therefore, in addition to using common feature algorithms, some new algorithms and combination algorithms can also be tried, such as applying deep learning to the implementation of classifiers or combining multiple algorithms [26] so as to extract more accurately and efficiently and identify the characteristics of the vulnerability text.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the project of Shanghai Philosophy and Social Sciences Plan (No. 2018BGL023).

References

- [1] Y. A. Basallo, V. E. Senti, and N. M. Sanchez, "Artificial intelligence techniques for information security risk assessment," *IEEE Latin America Transactions*, vol. 16, no. 3, pp. 897–901, 2018.
- [2] J. F. Luo and D. N. Fu, "Analysis of computer virus epidemic situation in December 2018," *Netinfo Security*, no. 2, pp. 85–85, 2019.
- [3] U. K. Singh, C. Joshi, and N. Gaud, "Information security assessment by quantifying risk level of network vulnerabilities," *International Journal of Computer Applications*, vol. 156, no. 2, pp. 37–44, 2016.
- [4] N. Abu-Ghazaleh, D. Ponomarev, and D. Evtyushkin, "How the spectre and meltdown hacks really worked," *IEEE Spectrum*, vol. 56, no. 3, pp. 42–49, 2019.
- [5] T. M. Conte, E. P. DeBenedictis, A. Mendelson, and D. Milojicic, "Rebooting computers to avoid meltdown and spectre," *Computer*, vol. 51, no. 4, pp. 74–77, 2018.

- [6] A. Shahzad, S. Musa, M. Irfan, and S. Asadullah, "Key encryption method for SCADA security enhancement," *Journal of Applied Sciences*, vol. 14, no. 20, pp. 2498–2506, 2014.
- [7] H. Yang, Y. Zhang, Y. Zhou, X. Fu, H. Liu, and A. V. Vasilakos, "Provably secure three-party authenticated key agreement protocol using smart cards," *Computer Networks*, vol. 58, no. 1, pp. 29–38, 2014.
- [8] K. B. Shi, *Research on Information Security Leakage Identification System Based on Machine Learning*, Fudan university, 2018.
- [9] G. Goth, "Functionality meets terminology to address network security vulnerabilities," *IEEE Distributed Systems Online*, vol. 7, no. 6, pp. 4–4, 2006.
- [10] H. Holm, M. Ekstedt, and D. Andersson, "Empirical analysis of system-level vulnerability metrics through actual attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 825–837, 2012.
- [11] C. Z. Cui, "Venustech's continuous construction of the information security ecological chain — analyze the information and cyber security strategy of Venustech," *Journal of Information Security Research*, vol. 3, no. 2, pp. 98–115, 2017.
- [12] J. Diamant, "Resilient security architecture: a complementary approach to reducing vulnerabilities," *IEEE Security & Privacy Magazine*, vol. 9, no. 4, pp. 80–84, 2011.
- [13] H. Yang and S. S. Lam, "Scalable verification of networks with packet transformers using atomic predicates," *IEEE/ACM Transactions on Networking*, vol. 25, no. 5, pp. 2900–2915, 2017.
- [14] Y.-H. Kim and W. H. Park, "A study on cyber threat prediction based on intrusion detection event for APT attack detection," *Multimedia Tools and Applications*, vol. 71, no. 2, pp. 685–698, 2014.
- [15] J. Kim, Y. Zhou, S. Schiavon, P. Raftery, and G. Brager, "Personal comfort models: predicting individuals' thermal preference using occupant heating and cooling behavior and machine learning," *Building and Environment*, vol. 129, pp. 96–106, 2018.
- [16] S. Martin, B. David, and H. Tracy, "Researcher bias: the use of machine learning in software defect prediction," *IEEE Transactions on Software Engineering*, vol. 40, no. 6, pp. 603–616, 2014.
- [17] A. S. A. Aziz and A. E. Hassanien, "Multilayer machine learning-based intrusion detection system," in *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, vol. 70, pp. 225–247, 2014.
- [18] X. He, S. Liu, and J. G. Jiang, "Comparative study of intrusion detection methods based on machine learning," *Netinfo Security*, vol. 18, no. 5, pp. 1–11, 2018.
- [19] M. H. M. Hanif, K. S. Adewole, N. B. Anuar, and A. Kamsin, "Performance evaluation of machine learning algorithms for spam profile detection on Twitter using WEKA and RapidMiner," *Advanced Science Letters*, vol. 24, no. 2, pp. 1043–1046, 2018.
- [20] P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. K. Kalita, "MLH-IDS: a multi-level hybrid intrusion detection method," *The Computer Journal*, vol. 57, no. 4, pp. 602–623, 2014.
- [21] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, pp. 296–303, 2017.
- [22] "China National Vulnerability Database of Information Security," *CNNVD vulnerability classification guide*, 2020, <http://www.cnnvd.org.cn/web/wz/bzqxqById.tag?id=3&mkid=3>.
- [23] L. Yang and S. Zhang, "A sparse extreme learning machine framework by continuous optimization algorithms and its application in pattern recognition," *Engineering Applications of Artificial Intelligence*, vol. 53, pp. 176–189, 2016.
- [24] W. Liang, W. Huang, J. Long, K. Zhang, K. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6392–6401, 2020.
- [25] P. Sunita and S. Jyoti, "A review of intrusion detection technique using various technique of machine learning and feature optimization technique," *International Journal of Computer Applications*, vol. 93, no. 14, pp. 43–47, 2014.
- [26] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 1–6552, 2020.