Hindawi
Journal of Sensors
Volume 2021, Article ID 1798256, 14 pages
https://doi.org/10.1155/2021/1798256

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]

[1]*Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan*
[2]*Department 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

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

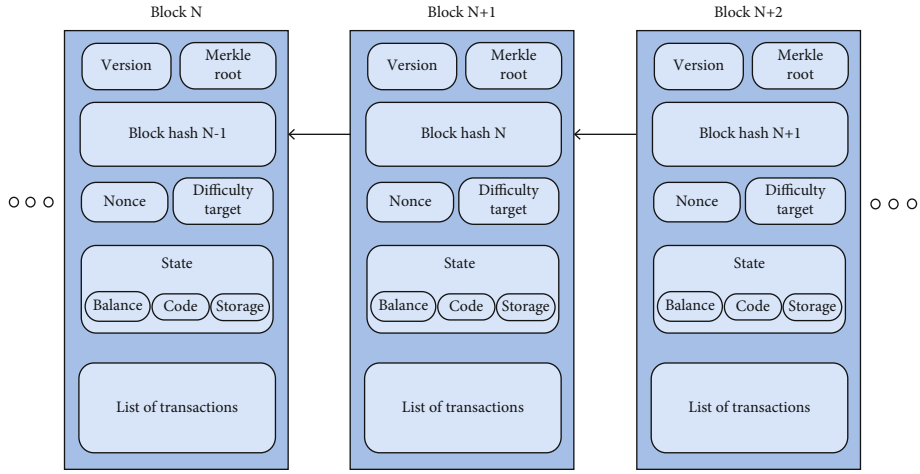

Figure 1: Blockchain structure.

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 promotes 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 (IoTs) 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 privacy. 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

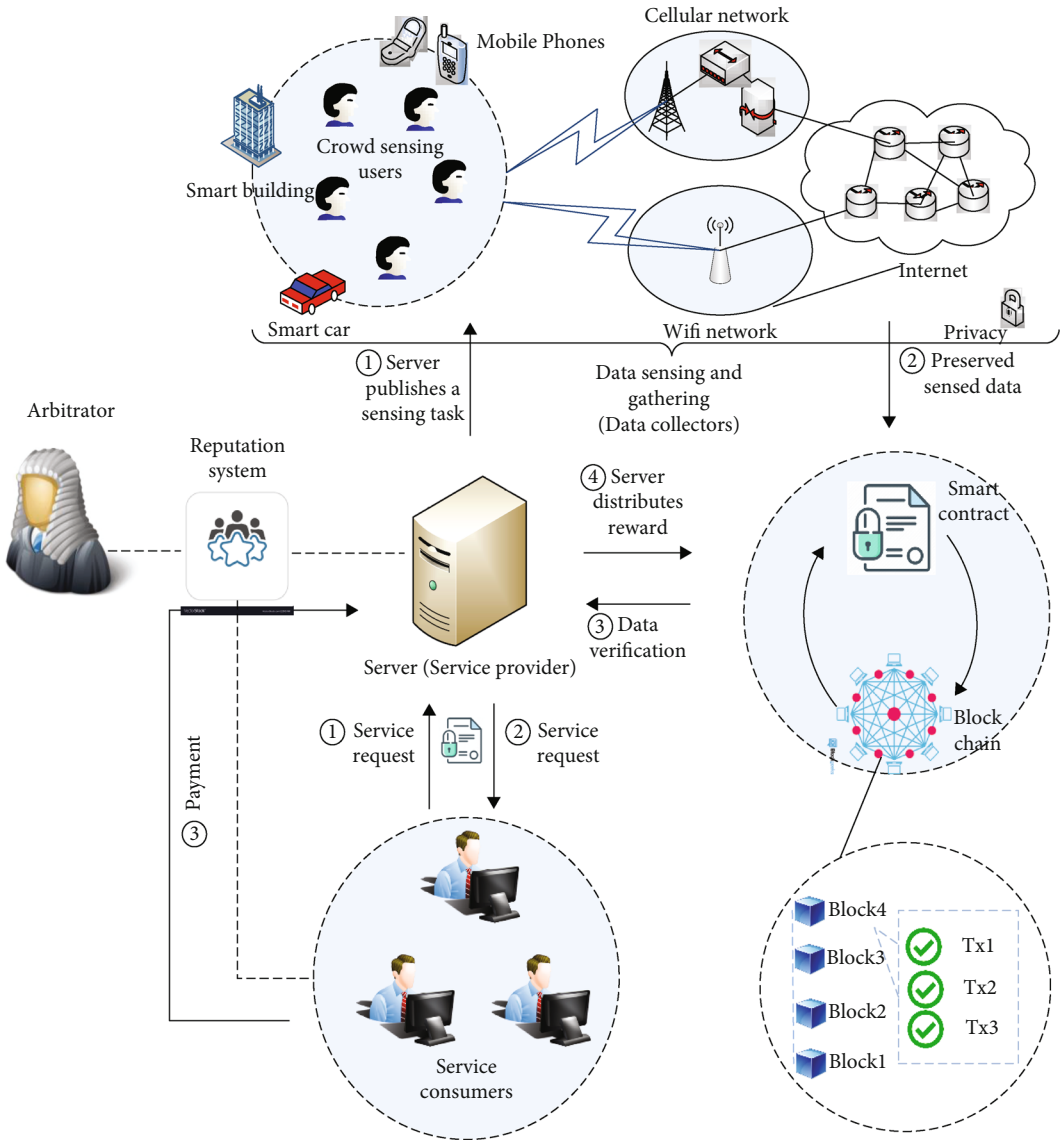

Figure 2: Blockchain-based incentive and reputation mechanism for CSNs.

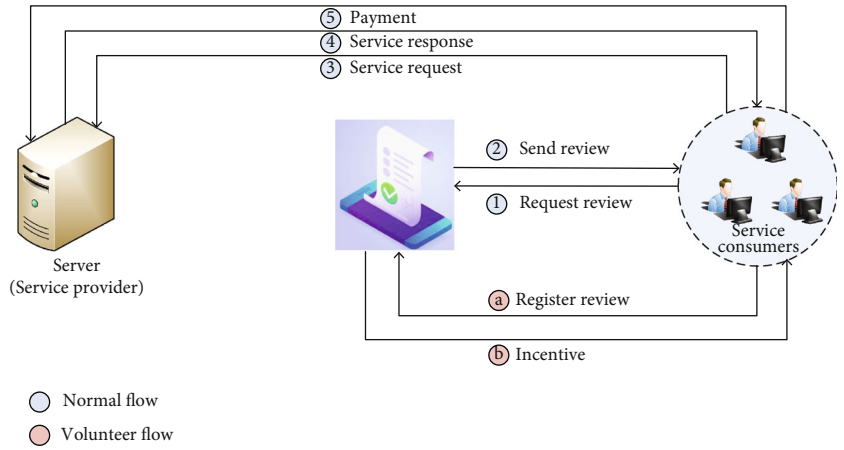

Figure 3: Reputation system for CSN.

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

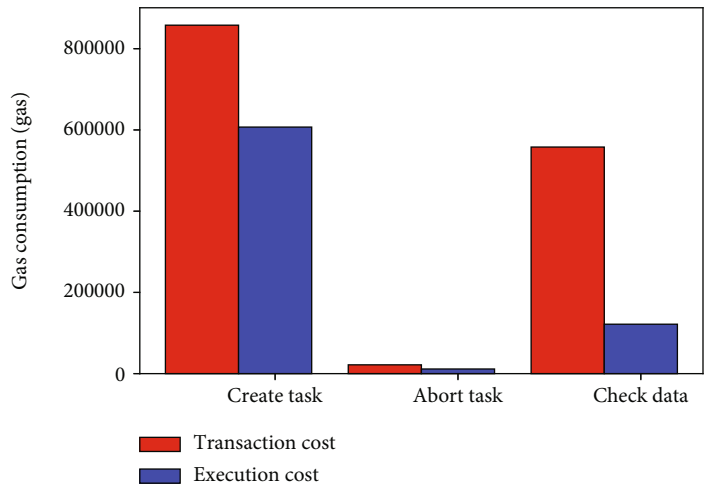

Figure 4: Gas consumption of service provider.

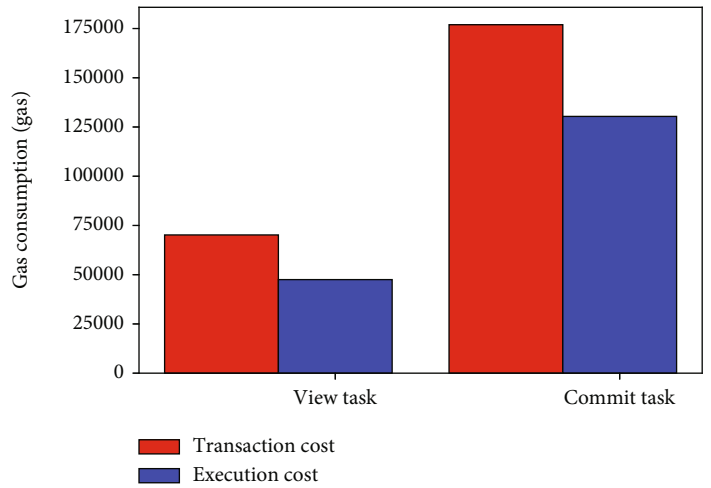

Figure 5: Gas consumption of data collector.

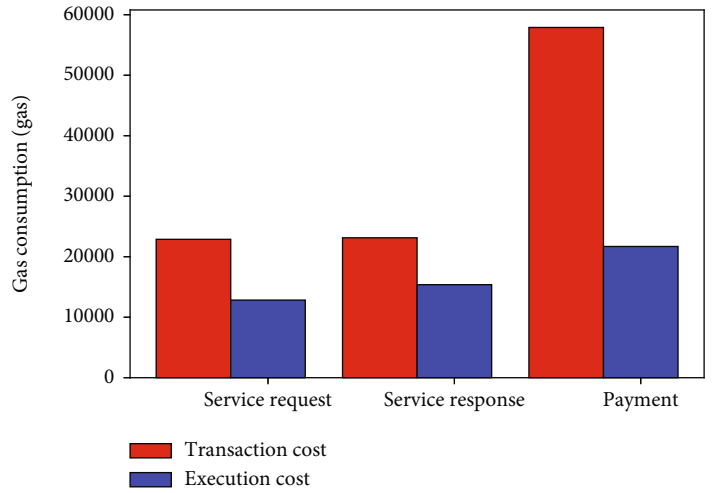

Figure 6: Gas consumption of service consumer.

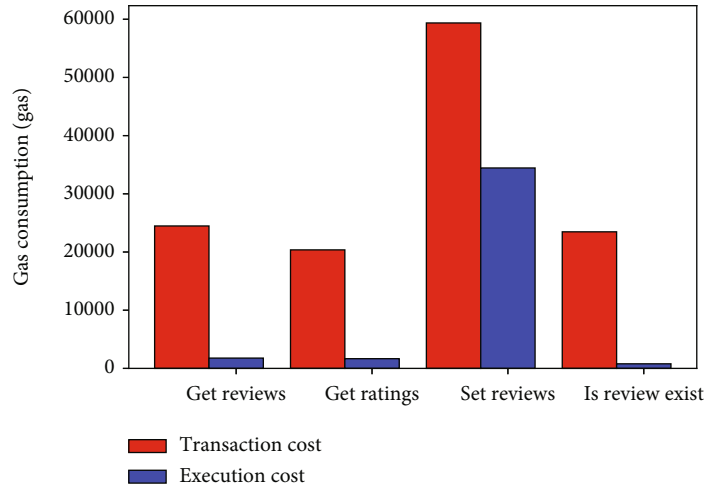

Figure 7: Gas consumption of review system smart contract.

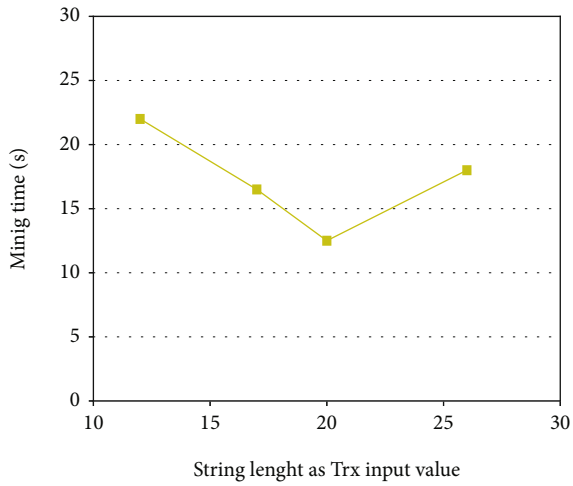

Figure 8: Mining time with different input values.

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,

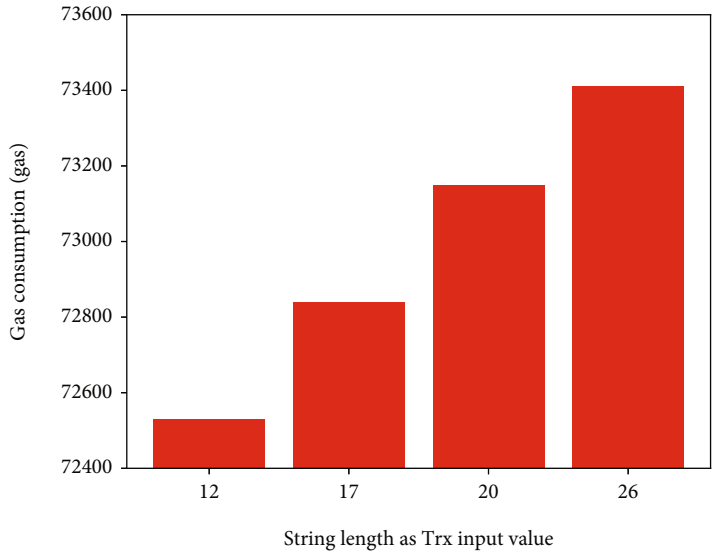

Figure 9: Gas consumption against different input values.

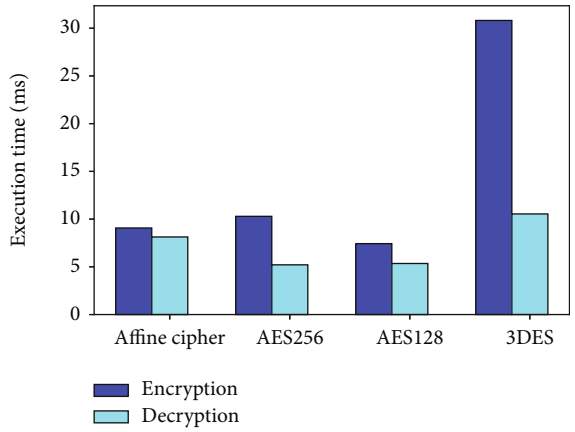

Figure 10: The comparison of execution time for affine cipher, AES256, AES128, and 3DES.

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. Giannetsos, 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. Raij, "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, "Participact: 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.