Security and Communication Networks

Blockchain Empowered Integration of Sensing, Communication, and Computing for the Internet of Things

Lead Guest Editor: Jianbo Du
Guest Editors: Zheng Chang, Lei Liu, and He Li

Blockchain Empowered Integration of Sensing, Communication, and Computing for the Internet of Things

Security and Communication Networks

Blockchain Empowered Integration of Sensing, Communication, and Computing for the Internet of Things

Lead Guest Editor: Jianbo Du
Guest Editors: Zheng Chang, Lei Liu, and He Li

Contents

A Management Specification for Data Sharing Security in the System Construction of Smart Mine
Haitao Wang, Lina Tan, Yang Zhang, Qiwen Gong, Shan Zhang, Yanan Ren, and Tao He
Research Article (13 pages), Article ID 1414530, Volume 2023 (2023)

Container Scaling Strategy Based on Reinforcement Learning
Huaijun Wang, Chenfei Zhang, Junhuai Li, Dan Bao, and Jiang Xu
Research Article (10 pages), Article ID 7400235, Volume 2023 (2023)

Design and Optimization of Blockchain-Based Distributed Data-Sharing System for Urban Rail Transit
Mo Chen, Hailin Jiang, Hongli Zhao, Huijun Zuo, and Qiang Zhang
Research Article (11 pages), Article ID 4211453, Volume 2023 (2023)

Detecting Fake Reviews with Generative Adversarial Networks for Mobile Social Networks
Zheng Qu, Qingyao Jia, Chen Lyu, Jia Liu, Xiaoying Liu, and Kechen Zheng
Research Article (11 pages), Article ID 1164125, Volume 2022 (2022)

New Constructions of Existential Unforgeable Aggregate Signature Scheme from CSP
Bo Mi, Yongxing Zou, Darong Huang, Yang Liu, and Lu Chen
Research Article (13 pages), Article ID 8954767, Volume 2022 (2022)

Privacy-Preserving Vertical Collaborative Logistic Regression without Trusted Third-Party Coordinator
Xiaopeng Yu, Wei Zhao, Dianhua Tang, and Kai Liang
Research Article (12 pages), Article ID 5094830, Volume 2022 (2022)

Compression Domain Reversible Robust Watermarking Based on Multilayer Embedding
Qianwen Li, Xiang Wang, and Qingqi Pei
Research Article (13 pages), Article ID 4542705, Volume 2022 (2022)

Hindawi
Security and Communication Networks
Volume 2023, Article ID 1414530, 13 pages
https://doi.org/10.1155/2023/1414530

Research Article

A Management Specification for Data Sharing Security in the System Construction of Smart Mine

Haitao Wang,[1] Lina Tan,[1] Yang Zhang,[1] Qiwen Gong,[2] Shan Zhang,[2] Yanan Ren,[2] and Tao He[3]

[1]*China Coal Energy Research Institute Co. Ltd, No. 66 North Yanta Road, Xi'an, China*
[2]*The School of Computer Science and Technology, Xidian University, Xi'an, China*
[3]*Institute of Intelligent Manufacturing, Wenzhou Polytechnic, WenZhou, China*

Correspondence should be addressed to Lina Tan; sabrina_tan2017@163.com

Received 27 July 2022; Revised 15 January 2023; Accepted 11 April 2023; Published 29 June 2023

Academic Editor: David Megias

With the development of Internet of Things technology and the informatization of the coal industry, various intelligent applications have emerged in the process of the system construction of the smart mine. During this process, data sharing is essential to the effective use of data resources in the smart mine. In order to improve the protection of coal mine data, this study proposes a set of management specifications for data sharing applied to the system construction of a smart mine to unify security standards in data storage and sharing. It standardizes the processes of data collection, transmission, and storage. We design three sub-specifications for these processes, namely, data source specification, data quality specification, and data storage specification. The data source specification specifies the data collection and transmission standards to improve the security and timeliness of data sharing. The data quality specification sets three evaluation criteria of integrity, accuracy, and timeliness according to the characteristics of each business system and data. The system ensures data quality during data sharing by governing and recording the data failing to meet the criteria. The data storage specification specifies the data storage protocol, data label, and data set restrictions. Only authorized platforms and users can share data and make use of data labels to search data efficiently. Finally, we constructed a coal mine data collection and analysis system. It can collect, manage, store, and safely share the real measured data from a certain colliery according to the specifications.

1. Introduction

With the rapid development of intelligence in the coal industry, the Internet of Things (IoT) has become the key technical support for the construction of intelligent mines. The innovative development of coal resources relies on big data technology. Coal mine data reflect the overall production process, production indicators, safety status, and other production information of coal mine. With the application of big data technology in smart mine, data become one of the most important resources. Colliery data have the following characteristics: first, the scale of the data is large; second, the data collection speed is fast; third, the value density of the data is low; and fourth, the data need high accuracy and strong timeliness. Data sharing is essential to the efficient use of data resources in smart mines. One of the biggest challenges of data sharing is to safely transmit the increasing amount of data. Data sharing is often accompanied by extraction, transformation, and loading processes. This means that data quality, data governance, and data security are particularly important. In order to realize the further progress of intelligent coal mine construction, data standardization has become a challenge.

In the operation of a smart mine, there are three different types of data sharing processes in the coal mine, as shown in Figure 1. First, all kinds of automation systems collect data and store it in the data storage platform. Second, the intelligent coal mine application extracts data from the storage platform and analyzes it. Finally, each coal mine aggregates the data collected by the automation system or from the data storage platform and submits it to higher management.

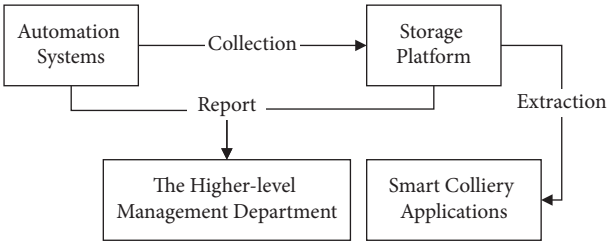

Figure 1: The data transfer processes in smart mine.

Since various automation systems belong to different businesses and have different functions, the type of data it manages and its granularity varies. Therefore, the data formats transmitted to the storage platform by each automation system are different. At the same time, there is a lack of uniform transmission protocols and standards for data sharing at all levels. As a result, storing and using coal mine data can often encounter problems such as low data accuracy, unguaranteed timeliness, data leakage, and difficulties in accountability. Specifically, there are four common problems, shown as follows:

(1) The format of the dataset is piecemeal, reducing data sharing security and timeliness, and the standardization workload is heavy. The data accessed by the intelligent coal mine big data platform is scattered on multiple devices. The file format and data format description of the sent data set are confusing and nonstandard when automation systems transfer data to the storage platform and the upper-level management department. The storage platform and upper management are unable to identify the integrity of the data, which is prone to data inconsistency caused by secondary delivery. Before implementing data from disparate business systems, the receiving unit must restandardize the data according to business demands. This restandardized process has resulted in an enormous workload for those responsible for data collection. It also led to delays in data collection and eventually no one wanted to take on the job.

(2) The lack of clear data quality descriptions makes the storage platform unable to guarantee the correctness of shared data. The coal mine automation system cannot describe data quality very clearly when uploading data. It makes the storage platform unclear about the quality of the data, making it difficult to ensure its correctness and unable to guarantee data standardization. This poses a potential hazard to future data applications. Problems with data quality can lead to duplication of data collection by the system, resulting in the reduction of data sharing, and it is difficult to form a virtuous circle.

(3) Coal mines have diverse production environments and equipment, and there is no uniform reference specification for data governance, especially for specific types of data. Coal mines have different business systems, and each business system corresponds to a variety of equipment. It is common for automated systems to generate abnormal data. The storage platform and data collection unit need to manage the error data submitted by each automatic system and perform different correction and annotation operations according to the type of error data. There is no dedicated governance for characteristic type data and sensitive data, which can easily lead to sensitive information leakage. Desensitized data are difficult to maintain data consistency and business relevance. Data governance is primarily done by people who do not have expertise related to mining. Data governance cannot achieve the expected results due to the lack of reference specifications for specialized governance methods for abnormal or irregular data or sensitive data.

(4) The platform does not have clear storage specifications, erroneous data are difficult to trace, and there are data sharing security issues. From production to the presentation of the final results of intelligent coal mine applications, coal data often go through multiple processes such as extraction, conversion, mapping, and reorganization. The platform does not select the appropriate data storage according to the business characteristics, and the systems easily access different levels of data. In these processes, security risks and errors such as data leakage, data tampering, data loss, data inaccuracy, data redundancy, and data expiration often occur. The lack of storage specification requirements for data storage retention times and record cyclic relationships makes it difficult to investigate errors and improve processes when these problems occur.

Because of the abovementioend problems, this study designs a specification for the data processing process in coal mines to unify security standards in data storage as well as sharing to improve the protection of coal mine data. This specification covers data collection, transmission, and storage in the process of unified data management in intelligent mines. It specifically includes data source specification, data quality specification, and data storage specification. It has the following attributes and functions:

(1) A data source specification: It describes the format of data transmission and file storage in the data collection process. It reduces the workload of coal mine workers, improves efficiency while reducing personnel, and reduces pretreatment work in the subsequent stage. The intention is to improve the security and timeliness of data sharing.

(2) A data governance specification: It helps software developers realize data governance without professional knowledge of coal mining and data mining. Design desensitization rules according to the data needs of different business units to improve the security of sharing special data.

(3) A data storage specification: It defines the data retention period of data storage and the mapping

format between recorded data. This specification makes it easier to track problems and improve the system when errors occur in production. Systems share data securely based on access rights for data.

This paper is arranged as follows. In Section 2, we review some relevant work. In Section 3, we design the top-level structure of the data management specification model. Then, three submodels are proposed, respectively, in Sections 4, 5, and 6. They are data source specification model, data quality specification model, and data storage specification model. In Section 7, we create a coal mine big data system to validate the utility of the specification and demonstrate the implementation of this data management specification. The study is concluded in Section 8.

2. Related Work

The authors in [1] provided a digital construction plan for coal mine big data based on life cycle management, which included technological approaches such as digital data collection, processing, and storage. It can also be used in other industries. The authors in [2, 3] used Internet of Things (IoT) technology to create a smart mining architecture. Their architecture includes data collection, data transfer, data storage, and intelligent applications. The authors in [4] presented a data platform system that combines digital technology, big data, and artificial intelligence. This data platform system can collect, transmit, store, and process smart mining data over the network. However, the main issues encountered in the development of smart mines, such as data transmission and storage efficiency, data quality, and data traceability, cannot be fully addressed in a single system.

Coal businesses employ IoT technology to construct smart mines in order to boost mine production and better manage coal mine big data. However, the problem of transferring huge amounts of data created by end devices has become an important issue that must be addressed. Edge computing is currently a very representative solution for reducing the Internet of Things data transmission delay [5–8]. In the studies of [9, 10], techniques for work assignment in edge computing systems are proposed. They carefully examined the trade-off between data transmission and computer resource allocation. Based on multihop vehicle computation resources, the authors in [11] suggested an adaptive algorithm offloading technique. The aim of these algorithms is to reduce task delays. Another solution to the problem of low-quality intelligent analysis findings produced by data noise in large data sets is to effectively minimize the data set size [12, 13]. The authors in [14] created an edge computing based system to handle data anomaly detection and analysis in underground mining. The edge devices were employed to do anomaly detection jobs, which increased efficiency. The authors in [15] present a study based on edge computing technologies that offered intelligent video surveillance for coal mines. FL-YOLO, a depthwise separable convolution and downsampling inverted residual block algorithm, was used in edge devices to identify security incidents. The authors in [16] developed an unloading task method that took into account network latency, wireless communication air rate, and computer resource consumption. To find the best option, they employed particle swarm optimization. The authors in [17] use federated learning in wireless edge networks to safeguard the privacy of user data, improving the performance of federated learning by jointly optimizing local accuracy and various resource allocation strategies. The authors in [18, 19] provide algorithms for the Internet of Things system's nodes. They evaluate the social relationships between nodes and partition the nodes to increase the Internet of Things' information transmission efficiency and network performance. Our specification is based on IoT devices and edge computing, standardizing data processing, designing anomalous data detection, and governance standards to improve data transmission speed and quality.

Various data standards are used in different fields to describe and manage data storage and transmission. For instance, in the field of geographical information, the International Standards Organization [20] provides a structure that describes the various steps involved in the data description, management, transmission, and sharing. In order to identify the types of errors in the metadata elements, the authors in [21] presented a method that can be used to improve the quality of data based on ISO 19157:2013. In the field of biology, the authors in [22] proposed data specification known as BIND was presented to describe and store the biomolecular information. In the field of medicine, various medical decision-making systems are based on the data collected and stored by multiple sources [23]. To improve the efficiency of telemedicine services, the authors in [24] developed a framework that standardizes the four processes involved in the collection, analysis, transmission, and decision-making of data. Due to the inconsistent nature of the data specifications in materials science, it is difficult to use them in deep learning. For addressing this issue, the authors in [25] created a data specification that is flexible, searchable, and formal. In the smart city, the data collected by the sensors will need to be stored and analyzed to improve the efficiency of the operations. The authors in [26] proposed an attributed-based specification that can be used to find and analyze the data. We proposed a data specification applied to the coal mining industry in the study of [27], but it is still not comprehensive, and this study makes further research on the basis of the study of [27].

3. Data Management Specification Model

This paper mainly discusses the specification of the data processing stage in coal mine, and the general framework is shown in Figure 2. The figure describes the direction of data flow. Data source access is to standardize the data collection behavior of each automation system at the source end, including data source, data format, and equipment information. Data transmission is a standard constraint on the transmission stage between different levels, mainly the specification of data transmission mode, transmission protocol, and data governance. Data storage standardizes data storage locations and storage media.

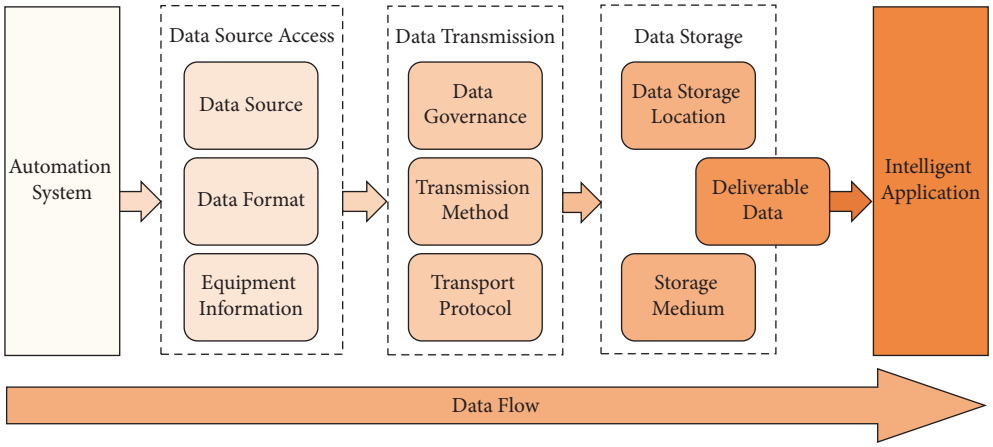

Figure 2: Overall framework of the data specification.

This section defines a data management specification model using unified modeling language (UML) based on the data source access, data transmission, and data storage parts of the abovementioned framework, as shown in Figures 3–6. It covers all data processing stages of smart coal mining, including data characteristics, data transmission, data quality, and data storage. The top structure of the data management specification model is depicted in Figure 3. It consists of three models: data source specification, data quality definition, and data storage specification.

The three models have the following connection. At first, the data source specification governs the data collecting and transmission method. This corresponds to the data source access, transmission method, and transport protocol. Second, the data quality specification outlines the data inspection and data governance procedures to be followed during the transmission process. This corresponds to the data governance module of the framework for data transfer. Third, the processed data is saved following the data storage specification. This requirement corresponds to the data storage module in the framework. Finally, intelligent coal mine applications retrieve and exploit the data.

(1) *Data Source Specification Model.* A full description of the data source is provided by the data source specification model. It specifies a hierarchical classification of the data. Some data must be recorded during the data collection and transmission procedure. The standard mandates documentation of the data source system and associated sources, as well as other pertinent and essential information, to permit traceability of issue data and accountability.

(2) *Data Quality Specification Model.* The data quality specification model is used to establish the data quality standards and assessment criteria for more advanced intelligent applications. Utilizing pertinent details like the data source system and source description, one may examine the data integrity, correctness, and timeliness efficiently. Furthermore, problematic or nonstandard data might be recognized, repaired, and handled by professional experts to raise the level of data quality.

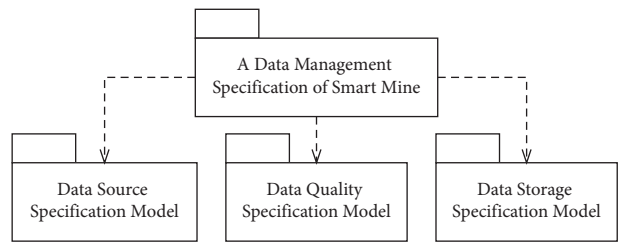

Figure 3: Data management specification model.

(3) *Data Storage Specification Model.* A detailed definition of the record information required to transmit data to the storage platform is provided by the data storage specification model. Data storage location, medium, and life cycle are all specified by the data storage specification model. The placement of the storage aids in making the data flow clear. Applications for coal mine intelligence can discover the information's source. The practitioner can more easily analyze the data lineage with its assistance. The life cycle assists in avoiding data duplication, enhancing the spatial exploitation of data storage, and providing greater support for intelligent applications.

4. Data Source Specification Model

The data source specification model is to standardize the process of data source acquisition and transmission. It unifies the data access process, classifies data hierarchically, and improves data sharing security. Figure 4 shows the data source specification model. During data collecting, the following details must be set at the same time: data source system, data source description, data transfer, identification, contact information, and references.

(1) *Data source system* gives specific information about the data source system, which is used to clarify the scope of business scenario requirements for data sharing and ensure that data usage is not beyond the authorized scope. For systems containing

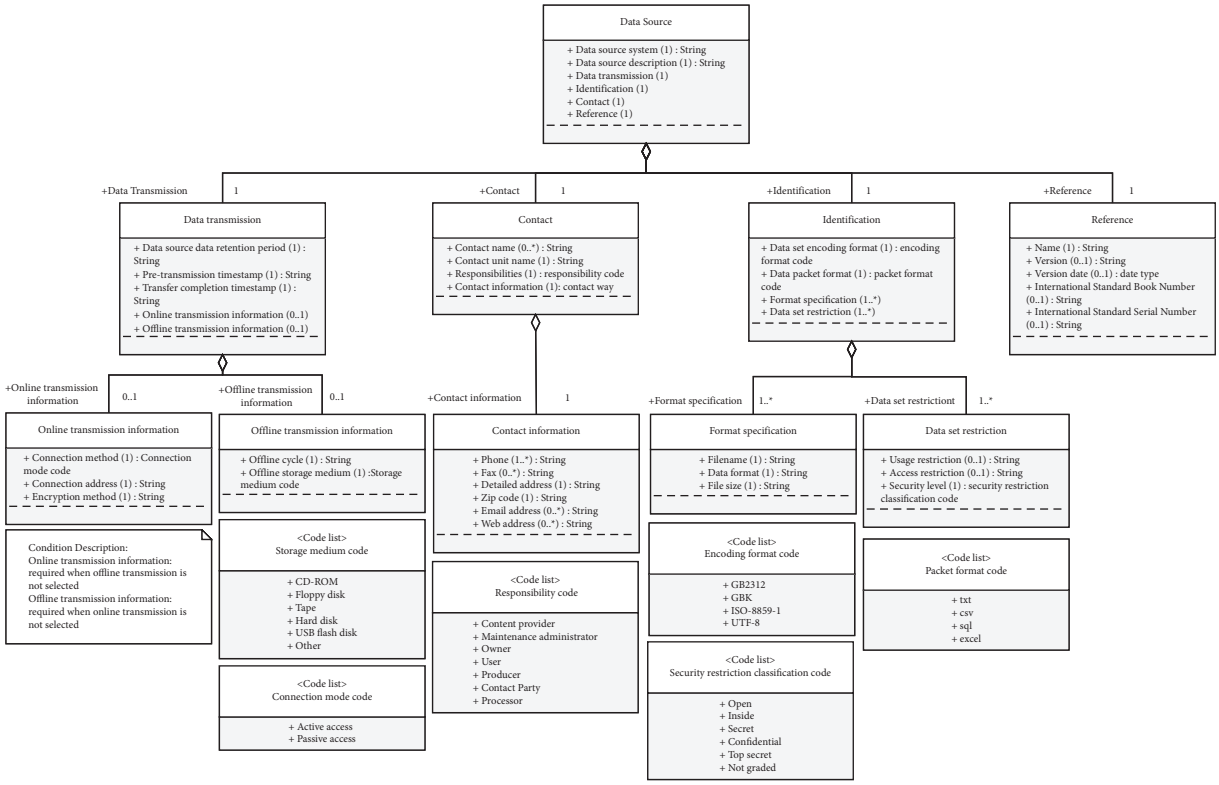

Figure 4: Data source specification model.

sensitive information, a database encryption system can be deployed. The information stored in the database is encrypted and stored, and an independent permission control system is used to realize the permission control of sensitive data access to ensure the security of its data. Data source system refers to the system from which the data are collected. We define five business layers for coal mine data, which are mine system, subsystem, device, subdevice, and measurement point. The data source system should include two layers: mine system and subsystem. For instance, common coal mine systems are coal mining system, excavation system, drainage system, ventilation system, transportation system, and electromechanical system. Subsystems are divided by area or function. For example, the subsystems of the main drainage system are the central pump house, the pump house below the adit, and the pump house in the 121-panel. In practice, mine systems and subsystems need to be modified according to the characteristics of the colliery. In order to standardize the processing of data, for the data sources of multiple business systems, the unified standard naming management of each business system and its equipment is realized through the master data naming specification. The naming rule of the full name of the mine is the abbreviation of the group company, the full name of the branch (optional), the scope of mining rights-coal mine. The naming rule of working face is working face number-function-working face. A specific example is 123 coal mining face.

(2) *Data source description* is a list of measurement points under the devices and their subdevices to provide the source of the data. As an example, some measurement points for a drive motor. The subdevices of the drive motor are motor, reducer, inverter, and high voltage switchgear. The measurement points of the motor are A phase winding temperature, B phase winding temperature, C phase winding temperature, motor front shaft temperature, motor rear shaft temperature, etc. For data from different automated systems, we use a data access method based on multiple data sources. A mapping relationship is established between the source and target data to achieve a unified naming and standardized description of the data set. Mapping the source data into a standardized format avoids repetitive human standardization work and improves the speed of data standardization. The source of the data can be located by keeping log records while it is being sent. As a result, personnel may inspect the associated data collecting devices and measurement sites to solve issues like data mistakes or inaccuracies when they arise.

(3) *Data transmission* describes the necessary information for data transfer and storage. It consists of the required field data and the retention period. To

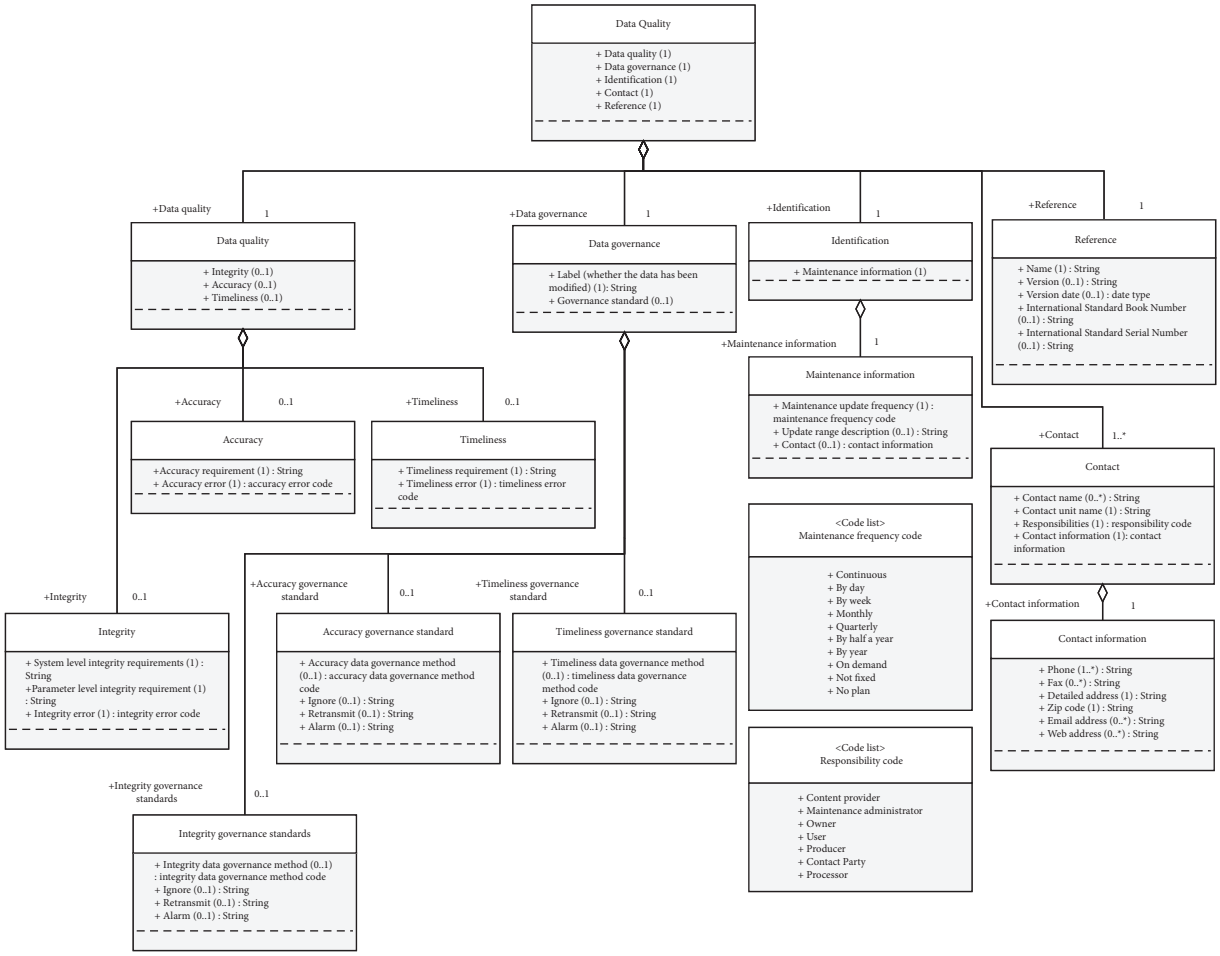

Figure 5: Data quality specification model.

prevent data loss and retransmission, the data source system needs to retain the data after successful transmission. Therefore, the retention time of the data source data are the length of time that the data need to be retained in the data source system after transmission. The system needs to record the time before and after data transmission to calculate the transmission delay and verify the data retention time. In the data transmission information, the transmission method must be online or offline information transmission. The online transmission information includes five fields: connection mode, encoding format, transmission protocol, connection address, and encryption mode. From the receiver's point of view, it can be divided into active and passive connection modes. The former model means that the data source opens the query port, and the latter mode means that the data source system sends the data directly to the receiver. If the offline transmission mode is selected, the offline period and offline storage media need to be recorded. That is, the system will record the frequency of offline transmission and the media used, such as weekly or monthly transmission using a hard disk. Encryption methods can be selected from one-way encryption, symmetric encryption, hash function, and digital signature. Users can select reasonable transmission modes and encryption methods according to data characteristics to enhance the security of sharing sensitive data. Recording the whole process of data flow helps to improve the data sharing log.

(4) *Identification* records information about the data format. The specification of data sets and packets prevents the computer from being able to read the code. The data set restrictions to limit the scope and manner in which the dataset can be used. This field ensures that only compliant personnel have access to authorized-mine data, improving the security of data. The identification also requires the data set to follow certain format specifications, reduce data parsing errors, and improve efficiency through a unified file naming format. The file head should be named "coal name; system name; data upload time." Among them, the data upload time refers to the time

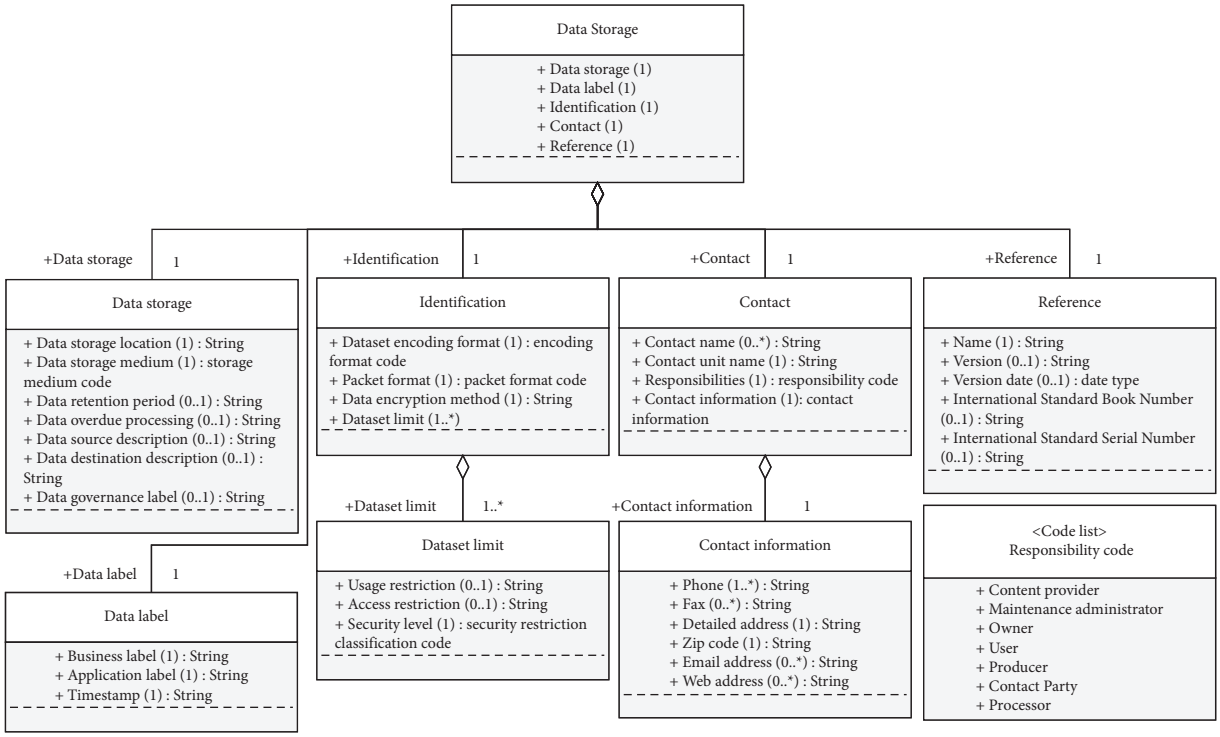

Figure 6: Data storage specification model.

of generating the data set file. The file body is a collection of measuring point data, and the data format is "measuring point; unit; upper range; lower range; upper alarm range; lower alarm range; data time."

(5) *Contact* records the contact person and contact unit of the data source system, specifying the institutional departments and responsibilities related to data sharing. If there is a problem with the source data, managers can quickly seek help through contact information.

(6) *Reference* records the industry management methods, professional theoretical knowledge of the coal industry, and relevant technical indicators related to this specification.

Data specification information can be set using XML files. Instance 1 shows a simple example of the data source specification model with XML format. It only gives partial information about the data source specification model.

5. Data Quality Specification Model

The coal data quality standard is described and evaluated using the data quality specification model, which also ensures the accuracy and consistency of the shared data. Figure 5 shows the data quality specification model, including the following modules.

Data quality is the specific criterion for describing and evaluating data. The specific content needs to be developed based on the advice of business experts and combined with the actual situation of the coal mine and the classification of data, taking into account the three attributes of integrity, accuracy, and timeliness.

To examine data integrity at the business level, it is necessary to consider the overall and local aspects separately. System-level integrity requirements describe the specific business information contained in the entire automation system, including system information, subsystem information, and equipment information respectively. For example, the ventilation system includes 3 ventilators, 2 vertical air gates, and 2 fan oil stations. The parameter-level integrity describes all data measurement points in the system. For example, the fan needs to measure the fan blade Angle, the winding temperature and bearing temperature related to the fan motor, the wind speed and efficiency of the fan, etc.

In addition, the accuracy requirements define the corresponding data type, data range, and data length of the measured point data. The data type ensures the accuracy requirements of the data. The data range allows for evaluating the data reasonableness. For example, if the data type is Boolean, then the data have no data range. If the data are of other types with a clear threshold range, then the data range needs to be specified according to the actual situation. The data range can be developed in a variety of ways, including the parameters of the equipment itself and the expert's estimate of the safety situation in the coal mine. For example, the upper threshold for the pool water level of the gas drainage system is 1.9 m and the lower threshold is 0.8 m. For the data with timeliness characteristics, the timeliness requirements are used to judge the quality of the data. Timeliness means that data will be recorded in chronological order and conform to certain rules of change. It is mainly

```
(1) <?xml version = "1.0" encoding = "UTF-8"?>
(2) <DataSource>
(3)    <dataSourceSystem>WJL-CFTS-2CCB</dataSourceSystem>
(4)    <dataSourceDescription>belt, drive motor and others</dataSourceDescription>
(5)    <dataTransmission>
(6)       <dataSourceDataRetentionPeriod>A Week</dataSourceDataRetentionPeriod>
(7)       <preTransmissionTimestamp>131974608035554296</preTransmissionTimestamp>
(8)       <transferCompletionTimestamp>131974608035554459</transferCompletionTimestamp>
(9)       <onlineTransmissionInformation>
(10)         <connectionMethod>Active Access</connectionMethod>
(11)         <connectionAddress>192.168.100.100:8080</connectionAddress>
(12)      </onlineTransmissionInformation>
(13)   </dataTransmission>
(14) </DataSource>
```

Instance 1: A simple example of the data source specification model.

judged and governed by data over a period of time. Timeliness requirements include time delay requirement and time sequence requirement. The time delay requirement is determined by the frequency of data acquisition. The optional parameters for the time sequence requirement are true and false. True means that the data has timeliness characteristics and needs to be governed using the time series algorithm. Data governance and maintenance are implemented according to integrity error codes. The error code of recorded data has a great impact on system error checking. For example, if the problem is caused by the application software, the data are likely to be skewed. Otherwise, the system should alert the contact to potential security vulnerabilities. At the same time, technicians shall check whether it is time according to the time stamp during data collection.

Data governance consists of a mandatory label and a mandatory governance standard. These mandatory governance standards come from integrity, accuracy, and timeliness. The label indicates whether the data have been modified and what specific modifications have been made. Data governance method, neglect, retransmission, and warning are four common mandatory fields covered by each governance standard. When the data are modified, the data governance method must be recorded. Data governance methods need to refer to expert experience and commonly used methods in related industries. Ignore implies that the inaccuracy is acceptable and should be disregarded. An essential field that contains an unfixable mistake has to be resent. If the data deviate greatly from the normal range, the alarm field will be enabled to inform the responsible person that there are security vulnerabilities in the system.

In the creation of specifications, many methods can be utilized to guarantee the data governance process. For sensitive data, common data desensitization methods are adopted for governance. For ordinary data, we use a density-based outlier identification approach to ensure accuracy. For time-series data, we use a time-series model to ensure timeliness.

The density-based outlier identification method is as follows. First, the data are grouped using quick search and density peak (DPC) [28] clustering algorithms. Then, any points whose distance from each center is more than or equal to the radius in the clustering procedure are picked as outlier candidate sets. Finally, an enhanced local outlier factor (LOF) [29] is employed to find outliers in the candidate outlier collection.

Formula (1) is used to locate cluster centers. Two concepts are defined. One is the sample i local density, which is denoted as ρ_i. Another is the shortest distance between the sample i and the location with a higher local density. It is denoted as δ_i.

$$\rho_i = \sum_{j \neq i} \chi(\mathrm{dist}(i, j) - d_c). \tag{1}$$

Here, $\mathrm{dist}(i, j)$ is the Euclidean distance between sample i and j. dc is a hyperparameter expressing cutoff distance. $\chi(x)$ is an activation function. $\chi(x) = 1$ when $x < 0$, else $\chi(x) = 0$.

$$\delta_i = \min_{j:\rho_j > \rho_i} (\mathrm{dist}(i, j)). \tag{2}$$

Here, δ_i is the one with the largest local distance among all samples. Those sites with larger rho_i and delta_i are selected as cluster centers.

In the second step, the improved LOF model $f(i)$ is utilized to calculate the degree of an outlier:

$$f(i) = \frac{1}{|N_k(i)|} \cdot \sum_{j \in N_k(i)} \frac{\rho_j}{\rho_i}, \tag{3}$$

$$N_k(i) = \{j \in S \mid \mathrm{dist}(i, j) \leq \mathrm{dist}_k(i)\}. \tag{4}$$

Here, ρ_i is the local density of sample i. $N_k(i)$ is a set composed of all samples in the k neighborhoods of a sample i. Formula (3) measures the extent of outlying. For example, if $f(i)$ greater than 1, the point i is located in a sparse area. It is an outlier. Otherwise, if $f(i)$ is less than 1, the local density of sample i is higher than its neighbors. This is the normal case. The aforementioned approach may be used to obtain the samples in the outlier candidate set S. Following the sorting of set, data governance may be applied to the first n outliers.

The data governance using time series model is as follows: for common time-series data, the time series algorithm autoregressive moving average model (ARMA) can be utilized. ARMA can assess whether the data include outliers based on a realistic value range. If the data are unreasonable, we will correct it.

For normal, stationary, and zero mean time series $\{x_t\}$, if $\{x_t\}$ is connected to the value and incentive of the preceding n steps, there is a general ARMA model (formula (5) [30]. The ARMA model comprises an autoregressive model (AR) and a moving average model (MA).

$$\begin{aligned}&\alpha_1 x_{t-1} + \alpha_2 x_{t-2} + \cdots + \alpha_n x_{t-n} + x_t\\&= \beta_1 n_{t-1} + \beta_2 n_{t-2} + \cdots + \beta_m n_{t-m} + n_t.\end{aligned} \tag{5}$$

Here, n and m are the order of autoregressive process and moving average correspondingly. The ARMA model is denoted as ARMA (n, m). If $n = 0$, the ARMA model becomes the MA model. If $m = 0$, this model is an AR model. $\alpha_i \in \mathbb{R}$ is termed the autoregressive coefficient and $\beta_i \in \mathbb{R}$ is the moving average coefficient. The series $\{n_t\}$ is the white noise sequence. Akaike information criterion (AIC) [31] is used to calculate the order of ARMA (n, m) model. The representation of AIC is given by the following formula :

$$\mathrm{AIC}(u) = \ln \widehat{\sigma}^2 + \frac{2u}{N}. \tag{6}$$

Here, $u = n + m + 1$ specifies the number of model parameters. N reflects the sample size and $\widehat{\sigma}^2$ is the error variance of the model. If the value of AIC is the least, then ARMA (n, m) is the best effective model for forecasting time series.

Identification describes the maintenance information of data quality. The maintenance personnel shall check and update the data quality requirements according to the maintenance and update frequency. When deploying new equipment, they need a set of requirements for timely updating data accuracy and timeliness according to the information of new equipment. *Contact* records the business experts consulted when setting up coal data quality and data governance methods. *Reference* mainly records the international standards referred to when specifying data quality standards and the instructions for equipment-related parameters.

6. Data Storage Specification Model

The data storage specification model describes the storage requirements in colliery data management, as shown in Figure 6. This facilitates the use of technologies such as storage encryption and backup to protect hierarchically classified data. It includes five modules: data storage, data label, identification, contact, and reference.

(1) *Data storage* defines data storage information. It covers the data storage location, medium, and retention time, among other things. The data storage location and the data storage medium are two required parameters that provide the particular URL route and storage media, respectively, by storing the precise URL path for improved traceability. For sensitive data, a good data storage medium needs to be selected. It also provides effective technology and management tools for data storage media to prevent data leakage due to improper use of media and improve the security of data sharing. It assists the system in identifying the precise flow of various business data by capturing the location of data. If it is necessary to retain the data for a certain period, the data retention period field needs to be set. This is an optional field to be set according to the actual requirements. The data overdue processing field is provided when the data are past due. Descriptions of data source and destination show the flow of data. The data source description specifies the data production system. It identifies the department responsible for the data. The data destination description specifies the access rights of each platform to different business data. Each platform should apply for data use to the data management department according to the authority to obtain data use authority and improve data sharing security. Data governance labels highlight the governance mechanism, whereas data labels primarily record the business system to which the data belongs. This is the distinction between the two.

(2) *Data label* includes a business label, an application label, and a timestamp. A typical mine industry business label can be divided into 4 layers: mine system, subsystem, equipment, and subequipment. Application label include worker type labels, device labels, disaster labels, operation labels, region labels, and system labels. Each piece of data can correspond to only one service label but can correspond to multiple application labels and provides a timestamp. Coal industry practitioners and IT industry practitioners can use business label and application label to rapidly query data.

(3) *Identification* shows the coding format, data packet format, and data encryption method for colliery data storage. Appropriate data encryption methods to protect the security of data sharing. To increase data security, it restricts the use of data sets and access personnel through data set constraints. It specifies the scope of data sharing scenarios and the rights holders of data sharing.

(4) *Contact* records the person responsible for storing the data. When the data are lost, we can quickly find the relevant person in charge to follow up on the situation.

(5) *Reference* includes the documents referenced and referenced in the process of formulating colliery storage standards.

7. Experiment

To demonstrate the validity and usefulness of the specification given in this work, we used data from the Wangjialing

coal mine to construct a set of coal mine data collection and analysis system. The system requires three identical computers to form a cluster, and the experimental settings are presented in Table 1. We obtained data from the Wangjialing coal mine's IoT devices with the coal company's permission. The data access process in the system is designed based on the data source specification, as illustrated in Figure 7. According to the data source specification model, the data access process must save data source information, data transmission, identification, contact, and reference. This contributes to data traceability and ensures the security of data sharing. In Figure 7, more detailed information on the data source system can be viewed by clicking on the description. For example, if you click on the task with the id is three, you can know that the coal mine is Wangjialing coal mine, the system is main ventilation monitoring system, and the subsystem is mine ventilation room. The data source data retention period is a week. The pretransmission timestamp is 182984608043, and the transfer completion timestamp is 182984608582. The data are transferred online, and the connection method is active access. The contact information of equipment contains the equipment manufacturer and phone number and so on.

Due to the wide range of data sources, including databases, files, and sensors, the data naming is not uniform. In order to unify the field names of coal mine data and record the data source system according to the data source specification, the data access process needs to implement the data mapping function. The data mapping function of the system is shown in Figure 8. After analyzing the data source file, select the data source file and the corresponding coal mine, system, subsystem, equipment, and field to make them correspond one by one. After completing these tasks, a mapping relationship will be generated between the source data and the target data, that is, a new data access task will be created. The target data can also form a uniform naming standard. The completed mapped data is encrypted by the data encryption standard (DES) algorithm and is then securely transferred to the storage platform.

In the data quality field, data governance is done as the data is being transferred. Data quality criteria for each type of data are defined based on the expertise of the experts and the device specifications. The data quality criteria for the 10 kV incoming cabinet are shown in Figure 9 by taking into account all factor types. This diagram shows the screenshot of the data quality standards of the coal mine data collection and analysis system. This figure shows the data quality specification model for the equipment 10 kV incoming cabinet, covering data quality, identification, and reference information. Completeness indicates this measurement point data for this device is present. Accuracy includes the data type and data range. 10 kV incoming cabinet only has an upper bound for every measurement point. The threshold range and reasonable range of the data determines how the data are processed, specifying whether the data should be governed, ignored, or alarmed. The version in the figure ensures the reference information of the data quality specification model. Each modification by the user will update the version number of the data quality standard and record the updated range description, the modifier, and the date of modification. By clicking on data governance, you can also see the corresponding governance methods and reference information referenced by the setting of the standard. By clicking on data governance, the governance method may also be seen. The data governance process is the next phase, which is determined by the data quality requirements. We have created comparable standards based on distinct parameter features. In order to verify the reliability of the data governance methods mentioned above, we have used the data of 10 kV incoming cabinet and motor as an example for illustration. The size of the dataset is 1000. For generic data (e.g., shaft temperature of the motor), we utilize the aforementioned density based outlier identification approach to find. The results are shown in Figure 10. Outliers that need to be handled are the data points in the red circle in the figure. The data are then adjusted using the mean, median, or other methods. For common time-series data such as current and voltage, the time series algorithm autoregressive moving average model (ARMA) is utilized. Figure 11 illustrates the results of residual analysis on line voltage data. The standardized residuals demonstrate that there is no shifting variation throughout time. The autocorrelation function (ACF) of the residuals suggests no autocorrelations. The Q-Q plot is a normal probability plot that demonstrates that the data conform to a normal distribution. The preceding research reveals that the ARMA model may be utilized to identify voltage data.

Table 1: Experiments parameters setting.

Parameters	Description
System	Windows 10
CPU	Intel core i7
GPU	NVIDIA GeForce GTX 1080
RAM	16 GB

As illustrated in Figure 12, certain data governance outcomes about the exhaust temperature of the pressure fan. It can be shown from the results that the specification can ensure data quality in the big data system. The governed data and associated information will be kept. The database will record the data storage location, retention period, overage processing method, data destination description, identification information, contact information, and reference information. For example, the data storage location is htpps://ip:9000/data/WJH-MVMS. The data retention period is a month. The data destination description is an algorithm platform. During data sharing, only the algorithmic platform and its users are authorized to access and use the data of this subsystem. The system will also tag the data with a data governance label, data label, and application label, recording the governance technique, business system, and data category. In addition, the system includes a security access control function. This module is responsible for authenticating the user's operation rights and only users with login rights can access and operate the data to achieve secure data sharing.

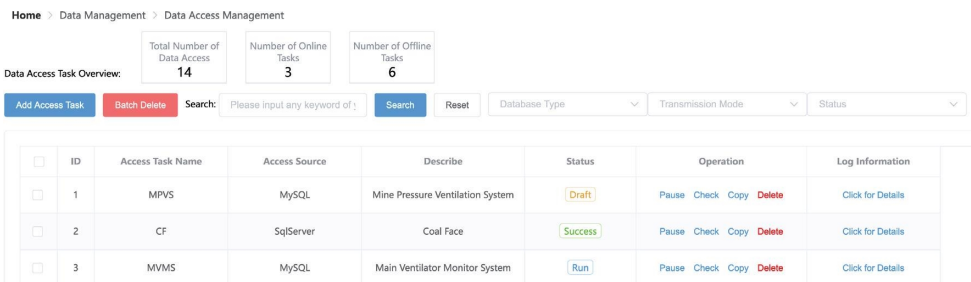

Figure 7: Screenshot of the data access function in the coal mine data collection and analysis system.

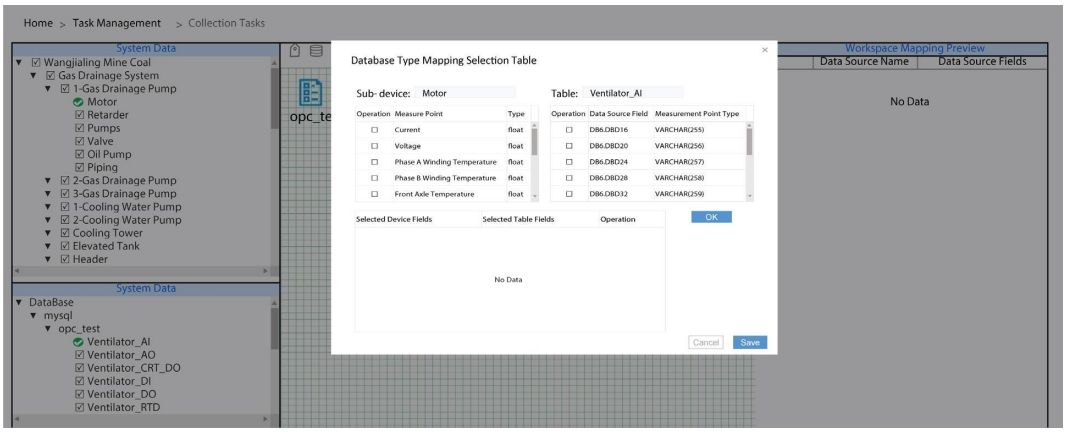

Figure 8: Screenshot of the data mapping process in the coal mine data collection and analysis system.

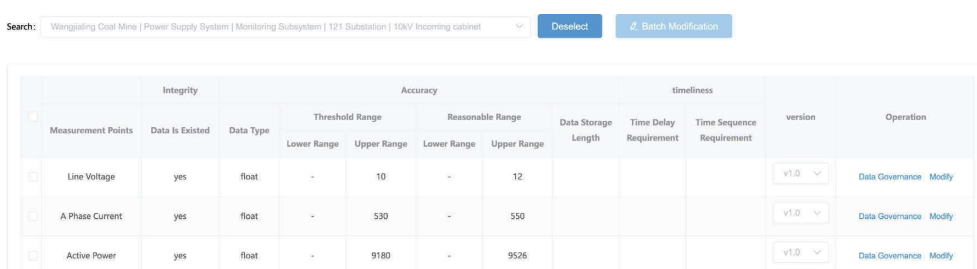

Figure 9: Screenshot of the system for 10 kV incoming cabinet data quality requirements.

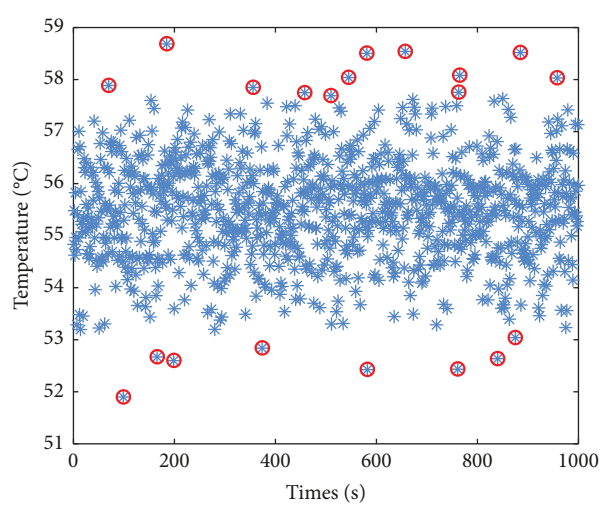

Figure 10: For the measure point of electrical machinery shaft temperature, a density-based outlier identification approach was used to identify the outliers and mark them with red circles to form the scatter diagram of the electrical machinery shaft temperature.

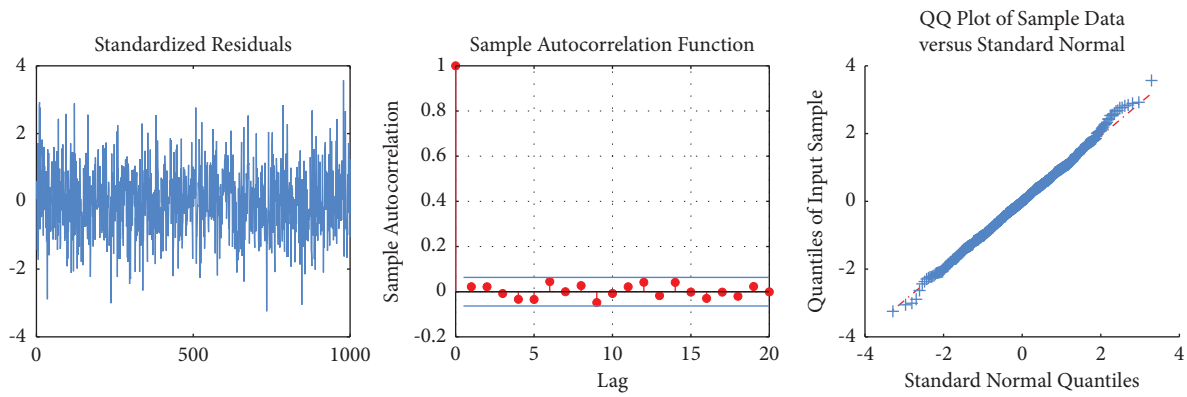

Figure 11: For the time sequence data of voltage, we use the ARMA model to judge the timeliness of the data and form a residual analysis diagram. It can be seen in the figure that the data are time series, and the ARMA model can be used to judge and govern the data.

Date	Exhaust Temperature		
	Data Governance?	Before Governance	After Governance
2022-03-07 15:28:20	yes	104.0	96.0
2022-03-07 15:28:19	yes	106.0	96.0
2022-03-07 15:28:18	no	95.8	95.8
2022-03-07 15:28:17	no	95.8	95.8

Figure 12: Screenshot of the governance results of the exhaust temperature of pressure fan in the data system.

8. Conclusions

The area of smart coal mining is growing quickly, and the enormous growth in data size creates a great demand for data management and data sharing. The lack of data standards causes inefficient use of computer and human resources and costly costs. To address these challenges, we have carried out the following: first, we offer a set of data specifications for data collection, transmission, and storage for big data practices in the coal mining sector. To improve the generality of data and the security of data sharing, our specification provides a complete data model that fills the gaps in data collection, transmission, governance, sharing, and storage according to the characteristics of the mining sector. Data are divided into business and application categories, and data tags are used to identify the category to which the data belongs, clarifying the scope of data sharing. Both those in the coal mining industry and those in the IT industry can easily find the data they need, allowing them to benefit from the specification. The standard sets up business-level classifications that allow employees to quickly track the source of anomalous data. Special governance rules for sensitive data ensure the security of sensitive data in the sharing process. Appropriate data encryption algorithms and transmission methods are selected according to the data transmission needs of different platforms to ensure the security of data sharing. Second, for the specification, we designed a short XML example for the data source model. All data criteria can be set and imported into the system based on this example. Third, we constructed a coal mine data collection and analysis system based on the standards of the data specification. The access, mapping, governance, sharing, and storage processes of data processing were implemented in the system. Experimental results show that the system verified the validity, usefulness, and security of the specification. Appropriate data encryption algorithms and transmission methods are selected according to the data transmission needs of different platforms to ensure the security of data sharing. In the future, we will try to combine microservices, privacy computing, and other technologies based on this specification to design multi-source data security sharing solutions that can meet cross-industry requirements.

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 that there are no conflicts of interest regarding the publication of this paper.

Authors' Contributions

L.T. and H.W. conceptualized the study; L.T., Y.Z., and T.H. proposed the methodology; H.W., S.Z., and Y.R. managed the software; Y.Z. investigated the study; L.T. gathered the resources; Y.Z. curated the data; H.W. and Q.G. wrote the original draft; Q.G. reviewed and edited the manuscript; and Q.G. visualized the study. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

The study was supported by Research and Development of Coal Mine Big Data Platform with Artificial Intelligence Applications' program of China Coal Energy Research Insititute Co. Ltd.

References

[1] L. Xianglan, "Digital construction of coal mine big data for different platforms based on life cycle," in *Proceedings of the 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, pp. 456–459, IEEE, Beijing, China, March 2017.

[2] Z. Qin, S. Chen, X. Xu, and M. Zhao, "Research on key technologies and system construction of smart mine," in *Proceedings of the 2020 5th Asia-Pacific Conference on Intelligent Robot Systems (ACIRS)*, pp. 116–121, IEEE, Singapor, July 2020.

[3] M. Zhao, "Technology of internet of things technology in the construction of smart mine," in *Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, pp. 289–292, IEEE, Chengdu, China, May 2020.

[4] X.-D. Hao and H.-W. Yang, "The research of the data platform system for the systemwide supervision and management of the intelligent mine in the opencast coal mine," in *Proceedings of the 2nd International Conference on Electrical and Electronic Engineering (EEE 2019)*, pp. 287–290, Atlantis Press, Penang, Malaysia, May 2019.

[5] L. Dong, M. N. Satpute, J. Shan, B. Liu, Y. Yu, and T. Yan, "Computation offloading for mobile-edge computing with multi-user," in *Proceedings of the 2019 IEEE 39th international conference on distributed computing systems (ICDCS)*, pp. 841–850, IEEE, Dallas, TX, USA, July 2019.

[6] P. Wang, L. Dong, Y. xu, W. Liu, and N. Jing, "Clustering-based emotion recognition micro-service cloud framework for mobile computing," *IEEE Access*, vol. 8, pp. 49695–49704, 2020.

[7] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: a survey," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1145–1168, 2020.

[8] L. Liu, J. Feng, Q. Pei et al., "Blockchain-enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor–critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.

[9] L. Dong, W. Wu, Q. Guo, M. N. Satpute, T. Znati, and D. Z. Du, "Reliability-aware offloading and allocation in multilevel edge computing system," *IEEE Transactions on Reliability*, vol. 70, no. 1, pp. 200–211, 2021.

[10] L. Dong, Q. Ni, W. Wu, C. Huang, T. Znati, and D. Z. Du, "A proactive reliable mechanism-based vehicular fog computing network," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11895–11907, 2020.

[11] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, pp. 1–14, 2022.

[12] L. Dong, Q. Guo, and W. Wu, "Speech corpora subset selection based on time-continuous utterances features," *Journal of Combinatorial Optimization*, vol. 37, no. 4, pp. 1237–1248, 2019.

[13] L. Dong, M. N. Satpute, W. Wu, and D.-Z. Du, "Two-phase multidocument summarization through content-attention-based subtopic detection," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 6, pp. 1379–1392, 2021.

[14] C. Liu, X. Su, and C. Li, "Edge computing for data anomaly detection of multi-sensors in underground mining," *Electronics*, vol. 10, no. 3, p. 302, 2021.

[15] Z. Xu, J. Li, and M. Zhang, "A surveillance video real-time analysis system based on edge-cloud and fl-yolo cooperation in coal mine," *IEEE Access*, vol. 9, p. 68482, 2021.

[16] Y. Meng and J. Li, "Task offloading and resource allocation mechanism of moving edge computing in mining environment," *IEEE Access*, vol. 9, p. 15534, 2021.

[17] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 56, no. 1-1, p. 1, 2022.

[18] X. Li, H. Qi, and J. Wu, "Node social nature detection osn routing scheme based on iot system," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 14048–14059, 2022.

[19] W. Yang, J. Luo, and J. Wu, "Application of information transmission control strategy based on incremental community division in iot platform," *IEEE Sensors Journal*, vol. 21, no. 19, pp. 21968–21978, 2021.

[20] ISO, *2003 Geographic Information-Metadata*, International Organization for Standardization (ISO), Geneva, Switzerland, 2003.

[21] M. A. Ureña-Cámara, J. Nogueras-Iso, J. Lacasta, and F. J. Ariza-López, "A method for checking the quality of geographic metadata based on iso 19157," *International Journal of Geographical Information Science*, vol. 33, no. 1, pp. 1–27, 2019.

[22] G. D. Bader and C. W. Hogue, "Bind—a data specification for storing and describing biomolecular interactions, molecular complexes and pathways," *Bioinformatics*, vol. 16, no. 5, pp. 465–477, 2000.

[23] G. Yu and J. Wu, "Efficacy prediction based on attribute and multi-source data collaborative for auxiliary medical system in developing countries," *Neural Computing and Applications*, vol. 34, no. 7, pp. 5497–5512, 2022.

[24] J. Wu, L. Chang, and G. Yu, "Effective data decision-making and transmission system based on mobile health for chronic disease management in the elderly," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5537–5548, 2021.

[25] Q. Qian, Y. Wang, and S. Zhao, "Materials data specification: methods and use cases," *Computational Materials Science*, vol. 169, p. 11, Article ID 109086, 2019.

[26] H. Moeini, W. Zeng, I.-L. Yen, and F. Bastani, "Toward data discovery in dynamic smart city applications," in *Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City*, pp. 2572–2579, IEEE, Sydney, Australia, Octber 2019.

[27] H. Wang, L. Tan, Y. Zhang et al., "A management specification for big data sharing in smart mine," in *Proceedings of the 2022 International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT)*, pp. 313–318, IEEE Computer Society, Los Alamitos, CA, USA, August 2022.

[28] A. Rodriguez and A. Laio, "Clustering by fast search and find of density peaks," *Science*, vol. 344, no. 6191, pp. 1492–1496, 2014.

[29] M. Breunig, H.-P. Kriegel, R. Ng, and J. Sander, "Optics-of: identifying local outliers," in *Proceedings of the 3rd European Conference on Principles and Practice of Knowledge Discovery in Databases*, Grenoble, France, September 2002.

[30] S. Lotfan and R. Fathi, "Parametric modeling of carbon nanotubes and estimating nonlocal constant using simulated vibration signals-arma and ann based approach," *Journal of Central South University*, vol. 25, no. 3, pp. 461–472, 03 2018.

[31] L. Ljung, "System identification," *Theory For The User*, vol. 12, 1999.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 7400235, 10 pages
https://doi.org/10.1155/2023/7400235

Research Article

Container Scaling Strategy Based on Reinforcement Learning

Huaijun Wang,[1,2] **Chenfei Zhang**,[1,2] **Junhuai Li**,[1,2] **Dan Bao**,[1,2] **and Jiang Xu**[3]

[1]*Collaborative Innovation Center of Modern Equipment Green Manufacturing in Shaanxi Province, Xi'an 710048, China*
[2]*Xi'an University of Technology, Xi'an 710048, China*
[3]*China National Heavy Machinery Research Institute Co., Ltd., Xi'an 710032, China*

Correspondence should be addressed to Junhuai Li; lijunhuai@xaut.edu.cn

Received 3 September 2022; Revised 8 October 2022; Accepted 13 October 2022; Published 26 May 2023

Academic Editor: Jianbo Du

Elasticity capability is one of the most important capabilities of cloud computing, which combines large-scale resource allocation capability to quickly achieve minute-level resource demand provisioning to meet the elasticity requirements of different scale scenarios. The elasticity capability is mainly determined by the container start-up speed and container scaling strategy together, where the container scaling strategy contains both vertical container scaling strategy and horizontal container scaling strategy. In order to make the container scaling policy more effective and improve the application service quality and resource utilization, we briefly introduce Kubernetes' horizontal pod autoscaling (HPA) strategy, analyze the existing problem of HPA, and develop a container scaling strategy based on reinforcement learning. First, we analyze the problems of Kubernetes' existing HPA container autoscaling strategy in the scale-up and scale-down phases, respectively. Second, the Markov decision model is used to model the container scaling problem. Then, we propose a model-based reinforcement learning algorithm to solve the container scaling problem. Finally, we compare the experimental results of the HPA scaling strategy and the model-based reinforcement learning strategy with the results from the resource utilization of the application, the change of the number of pods, and the application response time; through the experimental analysis, we verify that the reinforcement learning-based container scaling strategy can guarantee the application service quality and improve the utilization of the application resources more effectively than the HPA strategy.

1. Introduction

The vigorous development of IoT cannot be achieved without the support of edge computing technology, which is needed for data fusion, data analysis, network security, and data security at the edge of the network [1]. Meanwhile, in the face of the growing data transmission and computation demands of IoT [2], edge computing can effectively cope with the lack of computing power of IoT devices themselves and fully alleviate problems such as network congestion [3]. For example, in a real industrial application scenario, real-time control of the production floor site is achieved by placing edge gateways inside the workshop. It is also possible to build an industrial control platform through the edge cloud and use the data analysis and decision-making capabilities provided by the platform to provide a basis for real-time control decisions [4]. In many fields such as industrial control, most of the services are deployed to the platform as containers. Considering the problems of scattered IoT devices, network heterogeneity, and limited computing node resources [5], it is important to design a reasonable and effective container resource scheduling mechanism in order to provide guaranteed application services to IoT devices.

Kubernetes, as the industry's leading container orchestration management system [6], is widely used in edge computing scenarios [7, 8]; however, the native container scaling policy and container scheduling policy of Kubernetes are too simple to meet the fine-grained resource scheduling requirements in edge computing scenarios. The HPA container scaling service implements container scaling mainly by measuring CPU and memory utilization, which has problems such as response delay and poor scaling timeliness and cannot meet the business requirements in edge

computing scenarios. The resource scheduling policy only collects the remaining CPU and memory metrics of nodes and calculates the priority of nodes with uniform weight values to complete container scheduling. The scheduling mechanism considers only a single indicator, and the weighting method is too simple, and it suffers from low utilization of cluster resources and resource scarcity, which cannot meet the individual resource requirements of applications in edge computing scenarios.

The operation of application container instances in a cluster consumes certain costs, including those caused by application response times exceeding the maximum threshold value, in addition to the cost of memory and CPU resources that the containers themselves need to consume. Therefore, a reasonable and effective container scaling operation affects the application service quality as well as resource utilization.

In recent years, with the rapid development of Internet technology, the number of network edge devices has been growing exponentially. Traditional centralized cloud computing exhibits various problems such as high latency, low bandwidth, and high energy consumption when dealing with these massive edge data, for which edge computing is proposed. Before the birth of edge computing, to make up for the shortcomings of traditional centralized cloud computing, the industry proposed various computing models, such as cloudlet [9], fog computing [10], and mobile edge computing [11], which have different architectures but all aim to make up for the shortcomings of cloud computing, meet the growing demand for data processing with the development of the Internet, and guarantee the quality of service for users [12].

In terms of energy consumption reduction and cost considerations, Wang and Wang [13] proposed a novel cluster-level control architecture to achieve coordination of energy consumption and performance of virtualized server clusters, and experimentally demonstrated that the approach can provide effective control of both application-level performance and underlying energy consumption. Chen et al. [14] proposed a premigration strategy based on three load dimensions, combining a hybrid genetic algorithm and knapsack problem to achieve multiple adaptations, and experimentally demonstrated that the algorithm can effectively improve resource utilization and reduce energy consumption. Jeong et al. [15] proposed an energy-efficient service scheduling algorithm for federated edge clouds, which aims to minimize service migration overhead and energy consumption, and experimentally demonstrated that the algorithm improves energy efficiency by 21% and reduces service violation rate by 80%. Feng et al. [16] studied the application of heterogeneous computing (HC) and wireless power transfer (WPT) to federated learning to address the performing efficient learning tasks on the devices and achieving longer battery life. Feng et al. [17] explored a min-max cost-optimal problem to guarantee the convergence rate of federated learning in terms of cost in wireless edge networks. The literature [18] proposes a task offloading scheme by exploiting multihop vehicle computation resources in VEC based on mobility analysis of vehicles. This offloading scheme can achieve significant improvement in terms of response delay by at least 34% compared with the other algorithms (e.g., local processing and random offloading). In mobile edge computing, Mao et al. [19] proposed a reconfigurable intelligent surface (RIS)-assisted secure MEC network framework to enhance the task offloading security. Wei et al. [20] designed a preprocessing approach to convert raw traffic data into available datasets for deep learning-based traffic classifiers, which tailors raw traffic data as training datasets by resolving its structure and content and pruning redundant information. The literature [21] model the resource allocation in vehicular cloud computing (VCC) as a multiobjective optimization with constraints that aims to maximize the acceptance rate and minimize the provider's cloud cost.

In terms of energy reduction and cost considerations, Wang and Wang [13] proposed a Co-Con cluster control architecture based on the feedback theory control to minimize cluster power consumption while ensuring the quality of service of applications in the cluster. Chen et al. [14] present a multiadaptive genetic algorithm-based resource policy for premigration scheduling of virtual machines, which effectively reduce the energy consumption of the cluster. Wu et al. [22] proposed Green Scheduling algorithm based on DVFS dynamic voltage frequency scaling technique and job priority, which can prevent overuse of resources and effectively reduce power consumption while meeting the minimum resource requirements of applications. Rossi et al. [23] proposed an interesting approach to solve the container scaling problem by constructing the state space and action space of the container scaling problem and used reinforcement learning to merge horizontal and vertical scaling. However, they did not consider the characteristics of the Kubernetes' environment.

The distinctive features of this work are as follows:

(1) We model the container scaling problem by the Markov decision process (MDP), which includes the design of state space, action space, and cost function.

(2) Based on model-basedreinforcement learning algorithm to realize the iteration of the cost value and container scaling strategy in the process of container scaling, we evaluate the best container scaling strategy by solving the optimal Q-value function in the iterative process.

(3) Simulations are executed with different system parameters to show the effectiveness of the proposed algorithm. Simulation results reveal that the reinforcement learning-based container scaling strategy can effectively guarantee the application service quality and improve the application resource utilization compared with the HPA strategy.

The remainder of this paper is organized as follows. In Section 2, we analyze the shortages of Kubernetes' own container scaling strategy in the changeable edge computing environment. In Section 3, we leverage the Markov decision model to describe the problem of container scaling policy mode. In Section 4, we propose the construction of the

Markov decision model. In Section 5, we present how to solve the optimal Q-value function in the iterative process of reinforcement learning, based on which the optimal container scaling policy is evaluated to achieve the optimal scaling of containers. In Section 6, we test and discuss the effect of two container scaling strategies in the same experimental environment. We conclude this paper in Section 7.

2. Kubernetes Autoscaling Strategy

The edge computing environment is characterized by low latency and large connections. The existing Kubernetes autoscaling policy cannot adjust to dynamic application load changes in a timely manner in an edge computing environment, and the application itself does not have high resource utilization.

In this section, we focus on the scaling strategy that comes with Kubernetes. First, we introduce the Kubernetes autoscaling service. Then, we study the scaling strategy and analyze the problems that exist in the expansion and scaling phases.

2.1. Kubernetes Autoscaling Service. The flow of a pod in Kubernetes from resource allocation to service access is as follows: the application uses a user-defined YAML file to fetch the corresponding image from the image repository; allocates the CPU, memory, and other resources required for its operation; and deploys the application to Kubernetes in the form of a pod. Based on different application scenarios, users can adjust the policy manually by adjusting the requests' and limits' parameters. The CPU is allocated in a lean configuration by default. When CPU resources are oversubscribed, if there are not enough resources on the host node, there will be a preemption phenomenon. Getting the entry address of an application requires creating a Service API object, where Ingress is an API object in the Kubernetes cluster that plays the role of a router, through which we can customize routing rules for forwarding, managing, and exposing services. The user distributes the route to the pod represented by the Service object through Ingress to access the application, and the specific request flow diagram is shown in Figure 1:

The Kubernetes autoscaling service, designed as a control loop, can be controlled periodically by the controller (Kube-controller-manager), and the period time can be modified with the horizontal-pod-autoscaler-sync-period flag (default is 30 seconds). During each cycle, Kubernetes' Control Manager queries the cluster for current resource utilization based on each specific metric defined by HPA. The control manager obtains the basic metrics from the resource metrics API or from user-defined APIs (including other metrics). For each pod resource metric value (e.g., CPU), the controller obtains data from the HPA policy for each pod targeted by the resource metric API. If target utilization is given, the controller will calculate the current utilization as a percentage of the resource requests for the containers in each pod. If the target raw value is defined, the raw metric is used directly. Then, the controller obtains the utilization on all target pods or the average of raw values (depending on the specified target type) and generates the ratio used to scale the number of copies required.

2.2. Kubernetes Autoscaling Strategy. Kubernetes comes with a container scaling policy, HPA, which requires the definition of an HPA object when creating automatic scaling behavior for a Pod replica set. To define an HPA object, you need to specify the parameters to ensure that the HPA works as intended, the main parameters are shown in Table 1.

Currently, the official version of Kubernetes only supports CPU as a scaling metric, and other types of scaling metrics are still in the testing stage. The automatic scaler HPA calculates the desired number of replicas by checking the CPU utilization of the corresponding Pod replica set and comparing it with a predefined target value, as shown below:

(1) Get the CPU usage of each replica in the replica set at the current time and sum up to calculate the CPU usage of the replica set, which is an absolute value, that is, how many units of CPU are used, and the usage unit is one thousandth

(2) Obtain the CPU allocation of each replica in the replica set, sum up and calculate the CPU allocation of the replica set, and calculate the CPU utilization of the replica set, which is calculated as the ratio of CPU usage to CPU allocation

(3) Calculate the desired number of replicas

(4) Check if the expected number of copies is greater than the upper limit MaxReplicas, and if it exceeds the upper limit, MaxReplicas will be the expected number of copies

(5) Check whether the expected number of replicas is less than MinReplicas, and if it is lower than the lower limit, MinReplicas is used as the expected number of replicas

In addition, to avoid system bumps caused by frequently triggering the scaling function, Kubernetes sets an energy-cooling time for autoscaling. By default, the interval between expansions is not less than 3 minutes, and the interval between scaling is not less than 5 minutes.

2.3. Problem Analysis of the Scale-Up Phase. Kubernetes requires a series of components to collaborate with each other to complete the scaling work, and the initialization time of pod t_{init} is calculated as follows:

$$t_{\text{init}} = \sum_{i=1}^{4} t_i. \tag{1}$$

When the application faces a large increase in requests, Kubernetes triggers the expansion and creates pods, and the time t_{init} is needed for the newly created pods to accept requests from users, as shown in Figure 2. At the moment of s1, the autoscaler checks that the load status of the pod replica set reaches the expansion standard and triggers the scale-up. At the

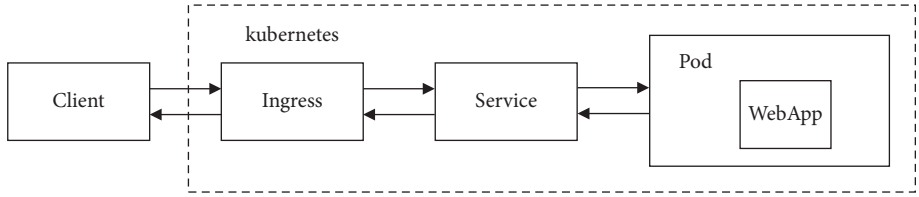

Figure 1: Web request workflow.

Table 1: HPA object parameters description.

Parameter name	Parameter value
MinReplicas	Minimum number of copies
MaxReplicas	Maximum number of copies
ScaleTargetRef	Scaling object
Target	Scaling indicators and target values

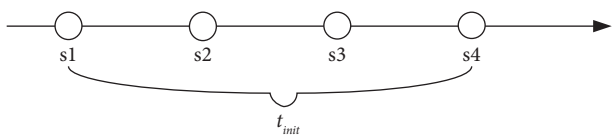

Figure 2: Scale-up time.

moment of s4, the scale-up is completed and the newly created replicas receive service requests. During the time of pod initialization, the replicas are overloaded and accumulate a large number of user requests, increasing user request time. Therefore, it is necessary to take the time of pod initialization into account when scale-up and prepare for the scale-up before the arrival of the load peak to reduce the response time of user requests, and thus ensure the stability of service quality.

2.4. Problem Analysis of the Scale-Down Phase. The purpose of the Kubernetes scale-down is essential to release the occupied resources by removing redundant pod nodes to improve the overall resource usage efficiency and reduce the overall application deployment resources. But in reality, although the application pod nodes are freed, the process only destroys the applications running on them, but the resources are not freed, as the underlying resource nodes are still within the Kubernetes resource pool. In a traditional private server room, the hardware purchased for the deployment of applications needs to go through preacquisition and shelving actions. Therefore, when the pod running on it is destroyed, it does not reduce the deployment and operation cost of these resources, and the only way to improve the overall utilization is to deploy other application services. In a public cloud environment, users only need to pay for these running resource instances, and when these idle nodes are higher than expected, they can effectively reduce operational costs by releasing these remaining nodes.

Kubernetes' flexible scaling is a natural fit with the public cloud's autoscaling, and Kubernetes' existing scaling strategy selects replicas to be deleted based on the priority of the replica state, unlike the preselection and preference process during expansion, which ignores the impact of deleting pods on cluster resources and actual business scenarios.

In order to achieve the scale-down of resource nodes, we expect to be able to concentrate as many pods as possible on certain nodes when scaling down and to shut down or delete the nodes of those pod nodes where fewer pod nodes are deployed by evicting the current node and calling the public cloud interface on it when it is in an unused state.

3. Container Scaling Policy Mode

The problem description for reinforcement learning using the Markov decision process consists of two main elements:

(1) Modeling the container scaling problem based on Markov decision models

(2) Based on reinforcement learning algorithm to realize the iteration of the cost value and container scaling strategy in the process of container scaling, we evaluate the best container scaling strategy by solving the optimal Q-value function in the iterative process

The model is shown in Figure 3.

3.1. Modeling the Container Scaling Problem Based on Markov Decision Models. Markov decision processes are discrete-time stochastic control processes that provide a mathematical framework for modeling decision problems. Markov decision models are usually represented by five tuples $\{S, A, P, C, \gamma\}$. S denotes the state space, here the state refers to the container state. A denotes the action space, here the container scaling action. P denotes the state transfer function. $P(s_t, a_t)$ denotes the probability that the state s_{t+1} is at the next moment after the intelligence executes the action a_t in the current state s_t. C denotes the immediate payoff function. $C(s_t, a_t)$ denotes the reward received by the intelligence after the execution of action a_t. γ denotes the discount factor, where $\gamma \epsilon [0, 1]$. When the discount factor is closer to 0, it indicates that the intelligence places more importance on the short-term cumulative reward value; when the discount factor is closer to 1, it indicates that the intelligence places more importance on the long-term cumulative reward value.

The Markov model for container scaling consists of three steps: state space design, action space design, and cost function design.

3.2. Iteration of Cost Values and Container Scaling Policies during Container Scaling Based on Reinforcement Learning. The process of an agent interacting with the environment in reinforcement learning can be viewed as a time sequence. The agent has a starting state s_t, then does an action a_t, the

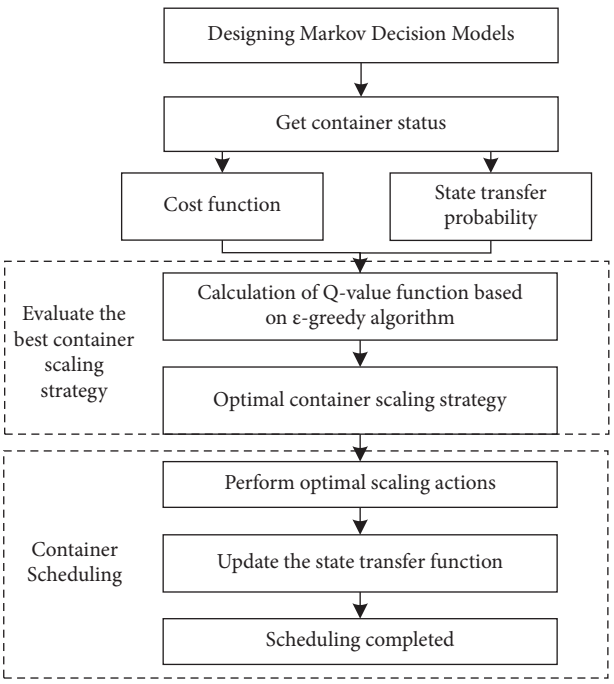

Figure 3: Container scaling policy mode.

environmental state changes to s_{t+1} and feeds back a reward r_{t+1}, and such interaction can go on forever.

In the reinforcement learning process, the change of state and the execution of a strategy have corresponding probabilities, indicating that they are all random events. The cumulative reward value obtained for each strategy execution trajectory is different, and the goal of reinforcement learning is to maximize the cumulative reward value by improving the strategy.

4. Construction of Markov Decision Model

4.1. State Space Design. The applications in the cluster are deployed and run in containers. The reinforcement learning intelligence perceives the state changes of the applications in the cluster environment and performs container scaling actions to effectively guarantee the quality of application services.

Define the state of the application at moment i as $s_i = (k_i, u_i, c_i)$, where k_i denotes the number of containers, and the range of k values is $\{1, 2, \cdots, K_{\max}\}$; $K_{\max}$ denotes the maximum number of copies of the application; u_i indicates the CPU utilization; and c_i indicates the amount of CPU computation granted to the container. Although u_i and c_i are real numbers, the discrete factors are set to disperse them for later strategy implementation. Assuming $u_i \epsilon \{0, \overline{u}, \cdots, L\overline{u}\}$ and $c_i \epsilon \{0, \overline{c}, \cdots, M\overline{c}\}$, $\overline{u}$ and $\overline{c}$ are suitable discrete factors. Define the state space S to store the state of all applications, which can be formulated as follows:

$$S = \{s_1, s_2, \ldots, s_n\}. \tag{2}$$

4.2. Action Space Design. The reinforcement learning intelligence senses the state of the application, performs container scaling operations, and optimizes the container scaling policy with the goal of minimizing expected costs.

For each state s in the application state space $S(s \epsilon S)$, there is a corresponding set of container scaling actions $A(s) \subseteq A$ that represent the container scaling actions performed by the intelligence in the application state s. A is the action space, defined as $A = \{-r, -1, 0, +1, +r\}$, consisting of 5 actions, where $+r$ indicates an increase in the amount of CPU resources and $-r$ indicates a decrease in the amount of CPU resources, i.e., +1 indicates a horizontal expansion to increase the number of container copies and −1 indicates a horizontal contraction to decrease the number of container copies, and $a = 0$ means to make no decision; action $A(s)$ is defined as follows:

$$A(s) = \{-r, -1, 0, +1, +r\}. \tag{3}$$

The action space A can be represented as follows:

$$A = \{A(s_1), A(s_2), \ldots, A(s_n)\}. \tag{4}$$

4.3. Cost Function Design. After a reinforcement learning intelligence makes an action a based on the current application's state s, the cost that the environment feeds the intelligence is also greatly related to the application's state s' at the next moment. We combine the different costs into a single weighted cost function, with different weights allowing us to express the relative importance of each cost term. Thus, we propose the immediate cost function $c(s, a, s')$ as a weighted value of several costs, representing the immediate cost spent to transform from state s to state s'. The weights of the immediate cost function range from $[0, 1]$, The mathematical expression of $c(s, a, s')$ is as follows:

$$\begin{aligned} c\left(s, a, s'\right) &= w_{\text{adp}} \frac{1_{\{\text{vertical-scaling}\}} c_{\text{adp}}}{c_{adp}} + w_{\text{perf}} \frac{1_{\{R(k+a_1, u', c+a_2) > R_{\max}\}} c_{\text{perf}}}{c_{perf}} + w_{\text{res}} \frac{(k+a_1)(c+a_2) c_{\text{res}}}{K_{\max} \bullet c_{\text{res}}}, \\ &= w_{\text{adp}} 1_{\{\text{vertical-scaling}\}} + w_{\text{perf}} 1_{\{R(k+a_1, u', c+a_2) > R_{\max}\}} + w_{\text{res}} \frac{(k+a_1)(c+a_2)}{K_{\max}}, \end{aligned} \tag{5}$$

where c_{adp} is the adaptation cost of the application to cover the cost of the application being unavailable when a certain container scaling operation is performed. c_{perf} denotes the cost of lost application performance, which is the cost to be paid when the response time of the application exceeds the response time limit $R_{\max}$. c_{res} is the cost of the resources used to run the application. The expense of this cost is proportional to the number of instances of the application and the share of CPU allocated to the container application. $1_{\{...\}}$ is an indicator function. w_{adp}, w_{perf}, and w_{res} are non-negative weights of different costs and $w_{\text{adp}} + w_{\text{perf}} + w_{\text{res}} = 1$. In this paper, we consider these three weight settings are equally important; so, we have $w_{\text{adp}} = w_{\text{perf}} = w_{\text{res}} = 0.33$. $R(k, u, c)$ is the application response time at state $s(k, u, c)$. In addition, the container scaling action a is decomposed into a horizontal scaling operation a_1 and a vertical scaling operation a_2.

5. Solving the Optimal *Q*-Value Function Based on the Iterative Process of Reinforcement Learning

When solving container scaling using reinforcement learning, the most important thing is how to solve the optimal Q-value function to evaluate the best container scaling policy to achieve optimal container scaling. There are many kinds of container scaling policies combining container state space and container scaling action space, and it is obviously not efficient enough to evaluate the policies by calculating the function values of each state-action pair one by one. This section focuses on computing Q-value functions using reinforcement learning algorithms.

First, we rely on the abovementioned system model and calculate the Q-value function directly using the Bellman equation:

$$Q(s,a) = \sum_{s' \epsilon S} p\left(s' | s, a\right)\left[c\left(s, a, s'\right) + \gamma \min_{a' \epsilon A(s_i)} Q\left(s_{i+1}, a'\right)\right] \forall s \epsilon S, \forall a \epsilon A(s), \tag{6}$$

where γ is the discount rate. The unknown transfer probability and unknown cost consumption can be estimated empirically.

Estimating the transfer probability $p(s'|s,a)$ can be translated into estimating the transfer probability of CPU utilization $p(u_{i+1} = u' | u_i = u)$, so the transfer probability can be written as the following expression:

$$\begin{aligned} p\left(s' | s, a\right) &= P\left[s_{i+1} = \left(k', u', c'\right) | s_i = (k, u, c), a_i = a\right] \\ &= \begin{cases} p\left(u_{i+1} = u' | u_i = u\right) & k' = k + a_1 \wedge c' = c + a_2, \\ 0 \quad \text{otherwise}, \end{cases} \end{aligned} \tag{7}$$

where $a = (a_1, a_2)$ refers to the container scaling operation, including horizontal scaling operation and vertical scaling operation, which is defined based on the updated number of containers (a_1) and the updated CPU share (a_2). Since the CPU utilization u is taken in a discrete set, we will briefly denote the transfer probability as $P_{j,j'} = P[u_{i+1} = j'\overline{u} | u_i = j\overline{u}]$. $j, j' \epsilon [0, \ldots, L]$. Definition $n_{i,jj'}$ stands for the number of CPU utilization changes when the application changes from state $j\overline{u}$ to $j'\overline{u}$ in time interval $\{1, \ldots, i\}$, where j and $j' \epsilon [0, \ldots, L]$. The estimated value of the transfer probability in time interval i can also be noted in the form $\widehat{P}_{j,j'} = n_{i,jj'} / \sum_{l=0}^{L} n_{i,jl}$. Then, we can estimate the direct estimation of $\widehat{p}(s'|s,a)$ by (5).

When we estimate the immediate consumption cost $c(s, a, s')$, we observe that the immediate consumption cost is composed of two components, known and unknown costs, which can be written as follows:

$$c\left(s, a, s'\right) = c_k(s, a) + c_u\left(s'\right), \tag{8}$$

where $c_k(s, a)$ is a known cost depending on the current state and operation, and in this paper, it takes into account the adaptation cost and resource cost. $c_u(s')$ denotes the unknown cost, which depends on the next state s'. $c_u(s')$ is determined by the performance loss because our assumed application model is unknown and we estimate the unknown cost $c_u(s')$ online. Thus, at time i, the RL intelligences can directly acquire the costs c_i and estimate the immediate cost $c_{u,i}(s')$ of the next state at time i, which can be represented as follows:

$$c_{u,i}\left(s'\right) = c_i + c_{k,i}(s, a). \tag{9}$$

Then, update the unknown cost $\widehat{c}_{u,i}(s')$ using $c_{u,i}(s')$, which can be formulated as follows:

$$\widehat{c}_{u,i}\left(s'\right) \leftarrow (1 - \alpha)\widehat{c}_{u,i-1}\left(s'\right) + \alpha c_{u,i}\left(s'\right). \tag{10}$$

The estimate of the unknown cost $\widehat{c}_{u,i}(s')$ is calculated based on the operation a in state s in (8). When the number of containers decreases, the CPU utilization increases and the CPU share decreases the cost spent to violate $R_{\max}$ is the expected cost of going from state $s = (k, u, c)$ to the next state $s' = (k', u', c')$. When updating $\widehat{c}_{u,i}(s'), \forall s \in S$, the following properties can be enforced:

$$\begin{aligned} &\widehat{c}_{u,i}(s) \leq \widehat{c}_{u,i}\left(s'\right) \forall \mathrm{k} \geq \mathrm{k}', u \leq u', c \geq c', \\ &\widehat{c}_{u,i}(s) \geq \widehat{c}_{u,i}\left(s'\right) \forall \mathrm{k} \leq \mathrm{k}', u \geq u', c \leq c'. \end{aligned} \tag{11}$$

From the above, the state transfer probabilities and cost functions can be obtained by estimation, so the Markov decision model for the container scaling problem in this paper is known. In other words, the reinforcement

learning intelligence is "fully observing" the environment with known changes in the environment. The Q-value function is then computed using the policy iteration algorithm in model-based reinforcement learning to evaluate the optimal container scaling action. The core idea of the policy iteration algorithm is to use dynamic programming to solve the problem, so this paper chooses the greedy method to implement the calculation of the Q-value function and evaluate the container scaling strategy by the Q-value function. The ε-greedy strategy idea is that the selection behavior of an individual in a state is such that it can reach the state with the largest state value among all possible subsequent states. The state value here refers to the container scaling cost. In the ε-greedy strategy algorithm, the intelligence randomly selects the action with probability ε and chooses the best container scaling action with probability $1-\varepsilon$. The strategy probability distribution can be written as follows:

$$\pi(s_t) = \begin{cases} \arg\max\limits_{a_t} & Q(s_t, a)\ p \le q, \\ a_{\text{rando m}} & \text{otherwise}, \end{cases} \tag{12}$$

where $a_{\text{rando m}}$ means a randomly selected action, $p, q \in [0, 1]$ and p value determines the probability of exploration of the intelligence; the larger p value is, the smaller the probability of exploration by the intelligence. Finally, the reinforcement learning update strategy algorithm is given as the Algorithm 1.

The abovementioned pseudocode briefly describes the whole process of learning and updating the container scaling policy. Firstly, the current container state s is obtained, and the state transfer probability P and immediate cost function c are estimated based on the container state s. Then, for each state s is refined to the specific container scaling operation, the Q-value function is calculated with the goal of minimizing cost consumption and the optimal container scaling policy is evaluated to achieve optimal container scaling.

6. Simulation Results and Discussion

6.1. Experimental Environment. The hardware environment is a PC with i5 processor and 16G RAM. The software environment is Windows 10 operating system, and the programming language is Python 3.0. The container Cloud Platform cluster environment is a Kubernetes cluster, which contains one master node and three node nodes. The open source edge computing framework EdgeX Foundry is deployed on top of the Kubernetes cluster as a container.

6.2. Container Expansion Experiment. The effects of the two container scaling strategies are tested in the same experimental environment. The experimental parameter settings we used and the observed metrics of the final experimental results mainly include the change in the number of pod copies, the change in application CPU utilization, and the change in application response time.

6.2.1. Implementation of HPA Container Scaling Policy. The HPA autoscaling policy is chosen as the comparison policy to achieve automatic scaling of php-apache container applications in a clustered environment by creating HPA objects. HPA works under dynamic random workload requests, increasing or decreasing the number of replicas based on CPU resource metrics. Implementing container scaling using HPA policies requires configuring HPA parameters and creating HPA objects.

This command contains the scaling object parameter, the CPU utilization target value parameter, the maximum number of copies parameter, and the minimum number of copies parameter. The HPA object parameters are shown in Table 2.

6.2.2. Implementation Process of RLS Policy. The policy implementation process requires setting several parameter values for implementing policy learning and updating, which are the application response time limit value, the scaling time interval, the range of the number of container instances, and the greedy policy exploration probability.

We reasonably assume that applications receiving a large number of requests in the edge computing environment have high requirements for real-time response to requests, so this paper sets the response time limit value $R_{\max}$ to be no more than 140 ms at maximum; the automatic scaling service of Kubernetes, which is designed as a control loop, has a cycle time setting of 30 s in the controller (kube-controller-manager). In the comparison experiment, we test the effect of two container scaling strategies (RLS vs. HPA) in three aspects: resource utilization of the application, change in the number of pods, and response time of the application, so the execution time interval of both HPA and RLS is set to 30 s; considering the size of the state space of the reinforcement learning algorithm, the range of the container instances number is set to the maximum value of 10 and the minimum value is 1, which can satisfy the optimization goal of reinforcement learning and also alleviate the problem of state space explosion.

The specific learning and updating process of the policy is listed as follows:

(i) Continuously obtaining the number of real-time container instances, CPU utilization, and application response time for the container during the time interval to determine the current state.

(ii) The selection of the best action is solved using a greedy algorithm, where the high probability of exploration determines whether the best action can be selected quickly. The container scaling strategy of reinforcement learning aims to obtain the best container scaling action in the process of continuous learning and exploration, with emphasis on the later exploitation effect. Thus, using smaller exploration probabilities will result in the best action obtained by exploration, which is more likely to be exploited the next time, and small probabilities may be slow to explore upfront, but the best action selection will be better as time grows.

(iii) After executing the optimal scaling action, the current state, i.e., the number of container instances, CPU utilization, and application response time, is

(1) Update estimates $\widehat{\mathbf{P}}_{\mathbf{j},\mathbf{j}'}$ and $\widehat{\mathbf{c}}_{\mathbf{u},\mathbf{i}}(\mathbf{s}_\mathbf{i})$
(2) **for** all $\mathbf{s} \in \mathbf{S}$ **do**
(3) **for** all $\mathbf{a} \in \mathbf{A}(\mathbf{s})$ **do**
(4) $Q(s,a) \leftarrow \sum_{s' \in S} \widehat{p}(s'|s,a) \cdot [\widehat{c}(s,a,s') + \gamma \min_{a' \in A(s_i)} Q(s',a')]$
(5) **end for**
(6) **end for**

Algorithm 1: Update strategy algorithm based on reinforcement learning.

Table 2: HPA object parameters.

Parameter name	Parameter value
MinReplicas	1
MaxReplicas	10
scaleTargetRef	Php-apache
Target	50%

Table 3: Reinforcement learning parameter.

Parameter name	Parameter value
Greedy strategy exploration probability	0.06
$R_{\max}$	140 ms
Time interval	30 s
Range of container instances	Rounded from 1 to 10

recorded as a way to update the state transfer probability and the record of the cost spent.

(iv) After each update of the state transfer probability, all the actions and state records need to be updated.

The abovementioned implementation process, with continuous cyclic learning at time intervals, and as time grows, the effective information increases thereby enhancing the effectiveness of the container scaling strategy. The relevant parameter values are shown in Table 3.

6.3. Experimental Results and Analysis. Container scaling is used to improve the CPU utilization of the application, to ensure the quality of service of the application with the least cost of pod containers, and to avoid taking up too many cluster resources.

The reinforced learning container scaling strategy can better adapt to dynamic load changes, the allocation of pod resources can respond quickly compared to HPA, the early stage is a continuous learning phase, the number of pod changes varies greatly, but later tends to be a smooth state, and can ensure the quality of service of the application, and does not occupy too many resources. But HPA for the request reduction, the number of containers cannot be reduced in time, occupying too many cluster resources, and the application itself has low CPU utilization.

To observe the difference in container scaling results under two container scaling policies with the same application request load. The experiments are conducted according to the parameters designed above to achieve container scaling under the HPA container scaling strategy and reinforcement learning-based container scaling, respectively. The effects of the two container scaling strategies are compared by observing the change in the number of instances of container applications, the change in CPU utilization of container applications, and the change in response time of container applications under the application request load.

Figure 4 shows the trend of the number of container instances. From Figure 4, it can be seen that the container application load requests are randomly and dynamically

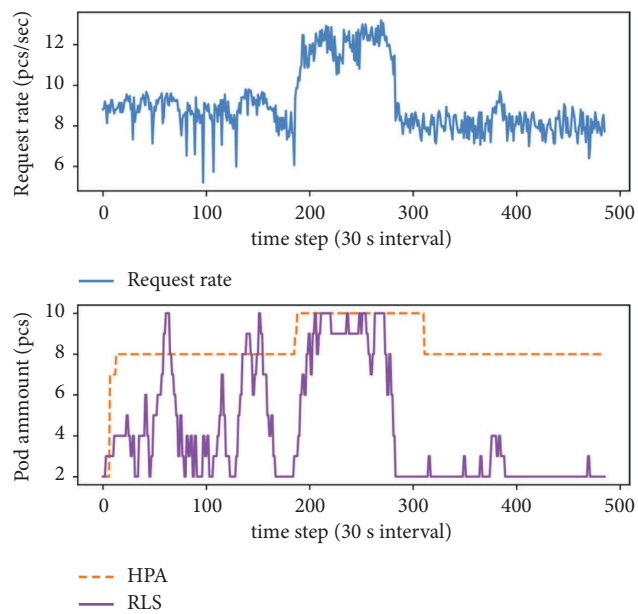

Figure 4: Trend of the number of container instances.

changing and have a tendency to rise and fall sharply. In this random dynamic trend, the HPA container scaling policy has a more stable trend to meet the application load request with more container instances throughout. At the same time, the red box in Figure 4 also shows that the HPA policy has a time lag problem when scaling up and down, while the container instances under the reinforcement learning policy can flexibly adapt to dynamic workload changes in a timely manner, and with more valid information, the container scaling is more effective.

Figure 5 shows the trend of CPU utilization of container application. In Figure 5, it is obvious that the overall CPU utilization of the application is low under the HPA container scaling policy, and under the RLS container scaling policy, the dynamic change is obvious in the early stage due to less effective information, and it tends to be stable and high in the later stage.

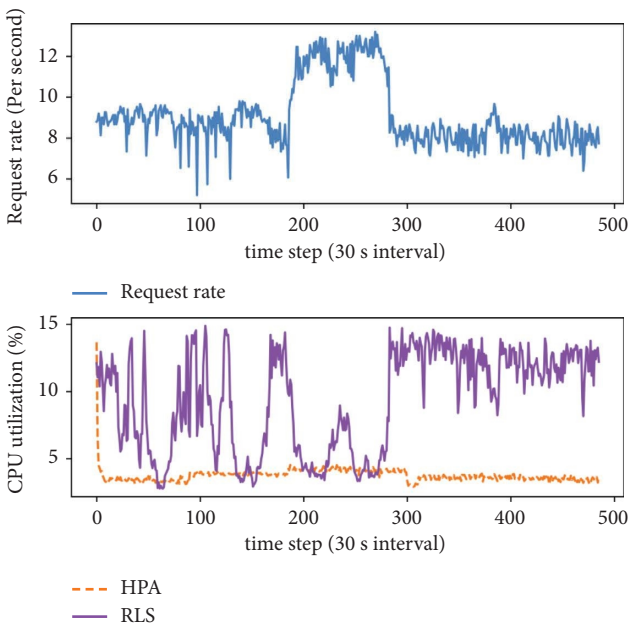

Figure 5: Trend of CPU utilization.

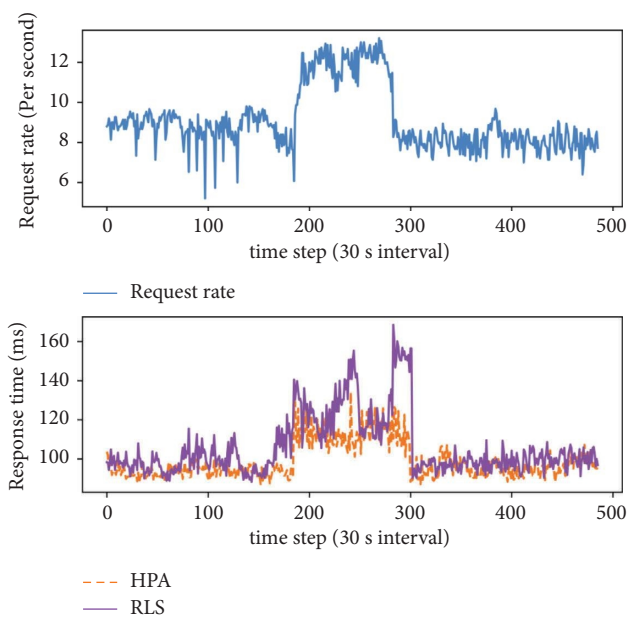

Figure 6: Trend of response time.

Figure 6 shows the trend of container application response time. In the early stage of RSL strategy, because the intelligent body does not interact with the environment for a long time, the effective information obtained is very little, and the optimal container scaling action is not obviously enough, so the application response time fluctuates a lot. In the later stage, with the continuous interaction and learning between the intelligence and the environment, the effective information obtained increases and the container scaling strategy is gradually optimized to select the container scaling action more accurately, thus meeting the application response time requirements.

Considering the limited resources in the edge computing environment, it is clear from the abovementioned analysis that the RLS strategy proposed in this paper has more advantages than the HPA strategy, which takes too much cluster resources as a condition to ensure the quality of service, and its timeliness is slightly lagged, its flexibility is poor, and its resource utilization is low. In contrast, the reinforcement learning strategy gradually optimizes the policy through continuous learning and decision making and finally guarantees the application service quality with less occupied resources, and it has high timeliness and high flexibility, which is more suitable for handling dynamic and randomly changing workloads in the edge computing environment.

7. Conclusions

This paper designs and implements a reinforcement learning-based container scaling strategy based on EdgeXFoundry, an edge computing framework, and Kubernetes, an open source container cloud platform, in conjunction with container scaling scenarios. Finally, we analyze the experimental results to prove that the reinforcement learning-based container scaling strategy can effectively guarantee the application service quality and improve the application resource utilization compared with the HPA automatic scaling strategy.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the National Key R&D Program of China (Grant no. 2018YFB1703003), Natural Science Foundation of China (no. 61971347), Key Research and Development Program of Shaanxi Province (2022SF-353), Shaanxi Water Conservancy Technology Project (2020slkj-17), and Collaborative Innovation Center of Modern Equipment Green Manufacturing in Shaanxi Province (Grant no. 112-256092104).

References

[1] J. Bin, J. Li, and G. Yue, "Differential privacy for industrial Internet of things: opportunities, applications and challenges," *IEEE Internet of Things Journal, to appear*, vol. 8.

[2] J. Fang and A. Ma, "IoT application modules placement and dynamic task processing in edge-cloud computing[J]," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.

[3] M. Min, L. Xiao, and Y. Chen, "Learning-based computation offloading for IoT devices with energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1930–1941, 2019.

[4] N. Soumyalatha and K. R. Manjunath, "Key technologies and challenges in iot edge computing," in *Proceedings of the 2019 Third International conference on I-SMAC*, pp. 61–65, Palladam, India, December 2019.

[5] C. K. K. Raymond, G. Stefanos, and P. J. Hyuk, "Cryptographic solutions for industrial internet-of-things: research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567–3569, 2018.

[6] P. Claus, "Containerization and the PaaS cloud," *IEEE Cloud Computing*, vol. 2, no. 3, pp. 24–31, 2015.

[7] N. Makris, V. Passas, and C. Nanis, "On minimizing service access latency: employing MEC on the fronthaul of heterogeneous 5G architectures," in *Proceedings of the IEEE International Symposium on Local and Metropolitan Area Networks*, pp. 1–6, Paris, France, June 2019.

[8] R. Morabito, "Virtualization on Internet of things edge devices with container technologies: a performance evaluation," *IEEE Access*, vol. 5, pp. 8835–8850, 2017.

[9] M. Satyanarayanan, P. Bahl, and R. Caceres, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Computing*, vol. 8, no. 4, pp. 14–23, 2009.

[10] F. Bonomi, R. Milito, and J. Zhu, "Fog computing and its role in the Internet of things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, pp. 13–16, Helsinki, Finland, March 2012.

[11] Y. Yu, "Mobile edge computing towards 5G: vision, recent progress, and open challenges," *China Communications*, vol. 13, no. 2, pp. 89–99, 2016.

[12] M. B. Yassein, O. Alzoubi, and S. Rawasheh, "Challenges and issues of fog computing: a comprehensive review," *WSEAS Transactions on Computers*, vol. 19, pp. 86–97, 2020.

[13] X. Wang and Y. Wang, "Coordinating power control and performance management for virtualized server clusters," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 2, pp. 245–259, 2011.

[14] S. Chen, J. Wu, and Z. Lu, "A cloud computing resource scheduling policy based on genetic algorithm with multiple fitness," in *Proceedings of the 2012 IEEE 12th International Conference on Computer and Information Technology*, pp. 177–184, Chengdu, China, July 2012.

[15] Y. Jeong, K. E. Maria, and S. Park, "An energy-efficient service scheduling algorithm in federated edge cloud," in *Proceedings of the 2020 IEEE International Conference On Autonomic Computing And Self-Organizing Systems Companion*, pp. 48–53, Washington, DC, USA, August 2020.

[16] J. Feng, W. Zhang, and Q. Pei, "Heterogeneous computation and resource allocation for wireless powered federated edge learning systems," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3220–3233, 2022.

[17] J. Feng, L. Liu, and Q. Pei, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 2687–2700, 2022.

[18] L. Liu, M. Zhao, and M. Yu, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Transactions on Intelligent Transportation Systems, to appear*, vol. 24.

[19] S. Mao, L. Liu, and N. Zhang, "Reconfigurable intelligent surface-assisted secure mobile edge computing networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6647–6660, June 2022.

[20] W. Wei, H. Gu, W. Deng, and T. C. Abl, "A lightweight design for network traffic classification empowered by deep learning," *Neurocomputing*, vol. 489, pp. 333–344, 2022.

[21] W. Wei, R. Yang, and H. Gu, "Multi-objective optimization for resource allocation in vehicular cloud computing networks," *IEEE Transactions on Intelligent Transportation Systems, to appear*, vol. 23.

[22] C. M. Wu, R. S. Chang, and H. Y. Chan, "A green energy-efficient scheduling algorithm using the dvfs technique for cloud datacenters," *Future Generation Computer Systems*, vol. 37, no. 1, pp. 141–147, 2014.

[23] F. Rossi, M. Nardelli, and V. Cardellini, "Horizontal and vertical scaling of container-based applications using reinforcement learning," in *Proceedings of the 2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*, pp. 329–338, Milan, Italy, July 2019.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 4211453, 11 pages
https://doi.org/10.1155/2023/4211453

Research Article

Design and Optimization of Blockchain-Based Distributed Data-Sharing System for Urban Rail Transit

Mo Chen,[1] **Hailin Jiang**,[1] **Hongli Zhao**,[1] **Huijun Zuo**,[2] **and Qiang Zhang**[3]

[1]*State Key Laboratory of Traffic Control and Safety, Beijing Jiaotong University, Beijing, China*
[2]*Unit 96901 of PLA, Beijing 100094, China*
[3]*Unit 61741 of PLA, Beijing 100094, China*

Correspondence should be addressed to Hongli Zhao; hlzhao@bjtu.edu.cn

Received 28 July 2022; Revised 4 September 2022; Accepted 13 September 2022; Published 15 April 2023

Academic Editor: Jianbo Du

With the wide application of data-driven intelligence technology, the management efficiency and quality of urban rail transit improve considerably. However, due to data privacy and security protection, a large amount of data is still scattered among operators or rail transit departments in the form of data islands. The data barriers between urban rail departments severely hinder the intelligent development of urban rail transit systems. In this study, we design a distributed data-sharing system based on blockchain for urban rail transit system. Data production node in urban rail department, such as servers in data centers, wayside equipment, and onboard equipment, can share their data in a distributed way. Blockchain provides audit and check functions to guarantee data-sharing security. We explore the data-sharing incentive mechanism which has an impact on sharing willingness of data production nodes. To maximize the individual utility of nodes, we formulate an evolutionary game model for data nodes with bounded rationality to adapt their sharing strategies. The uniqueness and stability of the equilibrium of the game are also analyzed theoretically. Extensive experiments are conducted and illustrated that data production nodes can share their data efficiently and safely in our proposed data-sharing system. Our proposed evolutionary game model can determine the most effective data-sharing incentive mechanism.

1. Introduction

A large amount of log data is generated during the daily operation of railways. Rail transit will generate train travel log data, passenger flow log data, fault alarm log data, line data, and so on. With the rapid development of rail transportation, the effective storage and analysis of the large amount of log data become a very urgent need. The analysis and processing of these data are of great significance to improve rail transportation capacity, strengthen rail transportation safety management, analyze accident causes, and reduce rail transportation operation costs. However, the data of rail traffic logs are stored in each independent department, which has strong confidentiality. The use and supervision of log data are very strict. If you want to use log data for fault analysis, accident tracing, passenger flow prediction, image recognition, and other scenarios, you will face many data security problems. Therefore, it is very important to ensure the safe sharing of log data and the confidentiality and privacy of the data.

Data-sharing technology will effectively solve the problem that the development of big data cannot be further promoted in the urban rail transit system. The traditional centralized data sharing provides a way to break the data barriers in the urban rail transit system industry. However, for the traditional data sharing, the data information of different application systems is often managed centrally. This information storage and access structure will bring a series of information security issues, such as the vulnerability of data center servers, which will lead to the risk of data leakage, and there is no unified standard for data management and data authorization. The problems of information security and computational efficiency exposed by the

traditional centralized data sharing and processing model have paid extensive attention.

To solve the above problems, we consider applying blockchain-based distributed data sharing. Nowadays, blockchain has been applied to digital finance, Internet of Things, intelligent manufacturing, supply chain management, digital asset trading, etc. The distributed data sharing based on blockchain has also been applied to some fields such as medical care. In terms of urban rail transit data sharing, a lot of research has not been carried out at home and abroad. Studying the urban rail transit data-sharing scheme based on blockchain can effectively promote the realization of more data-driven urban rail transit intelligent application scenarios and improve the intelligence level of urban rail transit.

We first design a distributed urban rail transit data-sharing system based on blockchain; then, an incentive model for users to participate in data sharing is defined using evolutionary game theory (EGT) [1]. EGT has been used widely to many studies, such as using prisoner's dilemma to study blockchain mining in bitcoin system. However, little research has been carried out on modeling proportion of users participating in data sharing. In our proposed model, each user has the choice to share data or not, leading to users to be divided into two groups: users who participate in data sharing and users who do not participate in data sharing, and users will play games with each other. Therefore, the game has four different strategies: participating user A, nonparticipating user A, participating user B, nonparticipating user B, and A and B are two sides of the game. The main contributions of this study are as follows:

(1) We design an urban rail transit blockchain-based distributed urban rail transit data-sharing system for users to share data

(2) We design an incentive mechanism to study the proportion of users' data sharing

(3) From the perspective of EGT, taking a pair of users as an example, we propose a model to study the impact of different incentive parameters on the final trend of data-sharing proportion of both sides of the game in this system.

The rest of this study is organized as follows. In Section 2, we discuss the related work. The design and implementation of the system are discussed in Section 3. In Section 4, we use the proposed game model to analyze the evolution of the proportion of users sharing data theoretically and numerically [2]. Then, in Section 5, we summarize this study.

2. Related Work

With the advent of the era of big data, the application of data-sharing technology has been extended to many fields such as machine learning, the Internet of Things, and medical care [3–5]. However, in the area of rail transit data sharing, a lot of research has not been conducted at home and abroad, and it is necessary to improve and innovate it by referring to data-sharing technology in other fields and combining its characteristics and needs.

2.1. Data Sharing. The traditional data-sharing system adopts a centralized service model, and data are generally centrally managed by a central server, which is not conducive to efficient and open data sharing. There are high security risks in the process of data exchange, leading to great concerns in the process of data sharing among various departments. Scholars at home and abroad have carried out a lot of research on how to build an efficient, secure, and private data-sharing system. Azaria et al. [5] proposed the MedRec medical data-sharing system, which is the first prototype data-sharing system in the medical scene. The big data-sharing platform presented by Yan [6] is composed of three major segments: management and operation system, data resource platform, and data application platform, which provides ideas for building a big data-sharing platform in China. Meanwhile, Poline et al. [7] proposed a data-sharing method in neuroimaging, which makes it easy for researchers to share raw, processed, and derived neuroimaging data, as well as appropriate metadata and provenance records and improves the reproducibility of neuroimaging studies. Feng et al. [8] proposed the use of federated learning to protect user privacy during model training. And the data-sharing approach proposed by Wang et al. [9] provides a solution for data manipulation based on structured data descriptions rather than raw data files. However, all the above data-sharing systems are designed based on distributed storage, and the rise of blockchain technology provides a secure privacy option for distributed data storage and sharing.

2.2. Data Sharing and Management Based on Blockchain. Zyskind et al. [10] proposed a blockchain-based personal data management system to prevent user privacy leakage due to personal data collection by third parties. A Hawk protocol based on blockchain smart contracts was designed by Kosba et al. [11] to guarantee the confidentiality of blockchain transactions and solve the problem of transaction privacy leakage. A blockchain application that can be used for IoT devices was presented by Dorri et al. [12] to address the data security and privacy issues in IoT scenarios. Linder [13] proposed to protect private files through public-private key encryption and use smart contracts to provide audit trails. Kostić and Tang [14] applied blockchain technology and big data analytics to the audit procedure. Ali et al. [15] offered a secure blockchain-based global named storage system. In terms of data management, Huang et al. [16] offered a blockchain-based IoT data sharing solution to solve three types of trustworthy problems in the process of IoT data sharing and management. Pinno et al. [17] designed an access control architecture for IoT and suggested a more resilient management approach. Di Francesco Maesa et al. [18] designed a blockchain technology-based access control approach for resources. Xu et al. [19] applied blockchain to a range of data management projects such as data valorization and sensitive information sharing. Krawiec et al. [20] presented the use of blockchain for healthcare information interaction. Xiong et al. [21] surveyed the latest schemes on secure and privacy-preserving medical data sharing in the

last decade and classified them into unlicensed blockchain-based and licensed blockchain-based approaches. Dubovitskaya et al. [22] later offered a permissioned blockchain-based sharing system for electronic medical data management and further improved the security and privacy protection mechanisms in the data-sharing system. Kuo et al. [23] proposed ModelChain, which combines privacy-preserving online machine learning with a private blockchain, for cross-institutional healthcare, addressing the security and robustness vulnerabilities of centralized architectures. Zhang et al. [24] investigated a blockchain-based data sharing framework for AI-driven network operations, using blockchain technology to establish a mutually trusted data-sharing framework to bridge the data barriers between different operators and implemented a prototype system based on a hyperledger structure. A secure data-sharing environment is created by combining access control and monitoring through data chains and behavior chains. Liu et al. [25] suggested a secure data-sharing scheme in the blockchain-enabled MEC system using an asynchronous learning approach.

Zhu et al. [26] proposed a blockchain-enabled distributed security scheme on communication-based train control system. On March 18, 2019, the first blockchain-based electronic invoice for rail transportation in China was issued at Futian Station of Shenzhen Metro, China, further securing the security and validity of metro invoice issuance by using the open and tamper-evident function of blockchain in data sharing and opening the precedent of blockchain technology application in the metro field.

3. Design of Blockchain-Based Data-Sharing Scheme for Rail Transit

To solve the above problems, we propose a blockchain-based data-sharing platform for rail transit, which can protect the security, privacy, and confidentiality of data sharing, and provide data sharing services to designated data requesters, while other participants cannot access unauthorized data content, this platform can promote the sharing of rail transit data, enhance data processing capability, and analyze data value, which is of great practical significance to the safe operation of rail transit and increase speed and efficiency.

3.1. Key Technologies. This platform is designed mainly using blockchain technology, which is used to record information and control access, and distributed storage technology, which is used to store files The platform is designed mainly using blockchain technology, which is used to record information and control access, and the Inter Planetary File System, which is used to store files.

(i) Blockchain: in 2008, Satoshi Nakamoto suggested the concept of "blockchain" in the "Bitcoin White Paper," and in 2009, he founded the Bitcoin social network and developed the first block, which is called the "genesis block" [27]. Blockchain system is a decentralized system. Each blockchain node sends messages to all other nodes, and each node decides the final policy based on all the messages it receives. Due to the high network latency in peer-to-peer networks, the order of transactions observed by each node cannot be exactly the same, so the blockchain system needs to set up a mechanism to agree on the order of transactions that occur at about the same time. This algorithm to reach consensus on the order of transactions within a time window is the consensus mechanism. And each block consists of a block header and a block body. The block header contains information such as the current block hash, the hash of the previous block, the version number of the block chain, the verification code of the block chain, and the timestamp of the block. The most critical information in the blockchain is called transaction, which is recorded by the data of the block. If node consensus fails, the blockchain rejects the transaction. Each device of rail transportation can store the log information summary in the blockchain, and complete the secure and trustworthy sharing of data through smart contracts.

(ii) The InterPlanetary File System: IPFS (InterPlanetary File System) is a decentralized file sharing platform that supports identifying files by their content. IPFS uses Distributed Hash Tables (DHT) to retrieve file locations and use them to communicate with nodes for connectivity. When a file is uploaded to IPFS, it is split into blocks, each containing up to 256 KB of data or links to other blocks, and each block is identified by a cryptographic hash, also known as a content identifier, which is calculated based on its content. Because IPFS uses content identifiers to identify, authenticate, and transfer blocks and files, it is particularly well suited for use with blockchains. In addition, a second, different files with the same hash cannot be easily created, so it is not possible to flood IPFS with files with a given target file identifier. In short, files provided via IPFS are easily verified, and it is difficult to block a compute node by providing a different file with the same name or identifier.

3.2. Blockchain-Based Data-Sharing Model for Rail Transit. The blockchain-based rail transit data-sharing platform includes four parts: rail transit data requester, rail transit data owner, rail transit decentralized data-sharing platform, and rail transit data source. As shown in Figure 1, the data requestors refer to relevant rail transportation departments, research institutes, upstream and downstream companies supplying rail transportation equipment, universities, etc., which have demand for data. They can be divided into several categories according to the application areas, such as train operation control, rail transportation equipment maintenance, and rail transportation passenger flow prediction. The data owners refer to the various rail transit departments that own rail transit operation data. They are responsible for the daily operation of rail transit, and the rail transit equipment of each department will generate a large amount of data. For example, onboard equipment generates

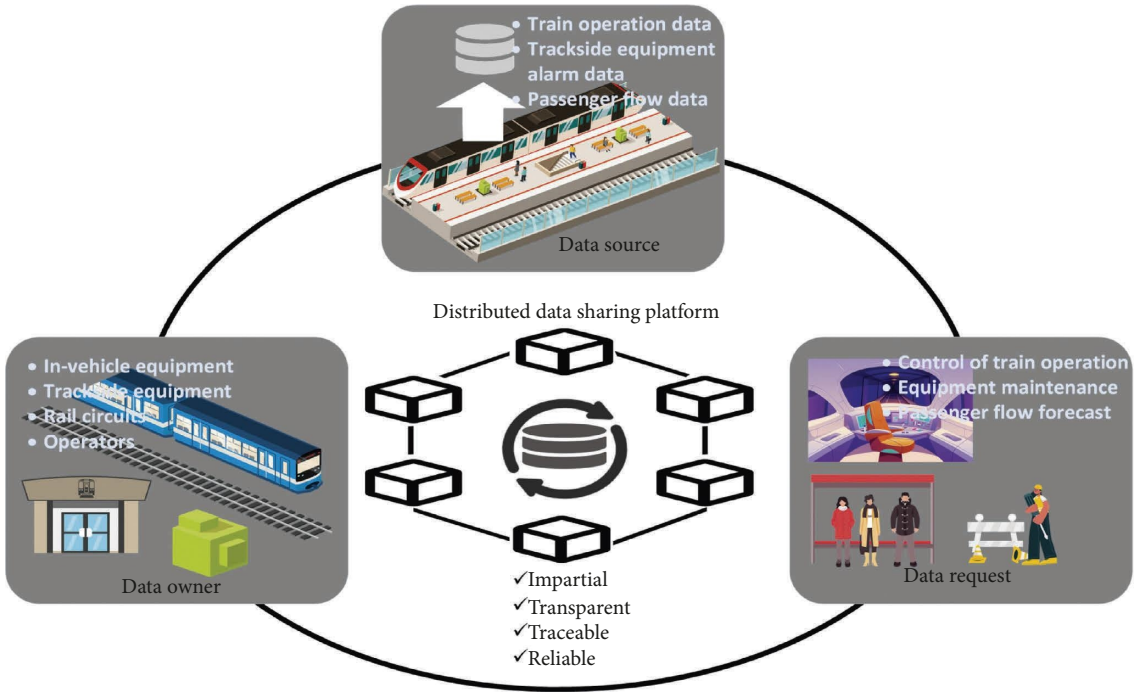

Figure 1: Blockchain-based rail transit data-sharing model.

train operation data, trackside equipment generates trackside equipment alarm data, and operators have daily new rail traffic flow data. Data source indicates the source of data, and the computer server provides data storage. It is held by the data owner.

In this model, the rail transit data owner releases data-sharing information through the blockchain data-sharing platform, and the rail transit data requestor initiates a data access request to the corresponding rail transit data owner according to its needs. After the rail transit data owner approves the access request from the data requester, the data requester can access the specified rail transit data content through the decentralized blockchain data-sharing platform. In addition, both parties can also complete data retrieval and data quality evaluation through the blockchain-based data-sharing platform. More importantly, the decentralized data-sharing platform can ensure the trustworthiness, transparency, and equality of the interaction between the two sides of rail transit data sharing. It creates a good data-sharing environment and protects the rights and interests of both parties sharing rail transit data.

Relying on blockchain technology, the decentralized data-sharing platform can meet the needs of rail transit data sharing for data trust, system security, and trustworthy expansion and has advantages that traditional data-sharing platforms cannot have.

3.3. Blockchain-Based Data-Sharing Access Control Method for Rail Transit. The meaning of access control is that when a requestor of rail traffic data requests access to the rail traffic log data, the data owner can give the specified data requestor access to his shared data by means of attribute encryption. Unauthorized users will not be able to access the data content. The data owner can protect the security and confidentiality of data sharing by keeping the data through the rail traffic data sharing platform.

The traditional public key encryption method is a coarse-grained access control with underground efficiency, which is difficult to adapt to the demand of selective sharing of rail transit data by data owners in rail transit data sharing. Therefore, this study proposes a data-sharing access control scheme based on blockchain and CP-ABE design. This scheme uploads the access policy with temporal attributes to the blockchain, and only data requesters whose node attributes satisfy the access policy within a specific time can obtain the decryption key. This scheme is suitable for solving the fine-grained control problem that exists in the rail transit data sharing environment. It can track the action records of rail transit data requesting nodes to publish request information and obtain access rights to rail transit data.

This access control method consists of three main participants: a track data owner, a track data requester, and a trusted key management center.

(1) DO: the track data owner, which is the unit or department that owns the track log data, is mainly responsible for publishing the metadata of the track dataset, setting the data-sharing access policy, and publishing the key and the cipher text based on the attribute encryption.

(2) DR: data requestor of rail traffic data is only the data requestor whose attribute set matches the data-sharing access policy and can access the specified dataset.

(3) AC: trusted key management center is responsible for generating public parameters and generating and

distributing keys for data owners and data requesters.

The CP-ABE algorithm in the blockchain-based data shared access policy for rail transit is divided into four parts.

(1) System initialization: the initialization is executed on the Trusted Key Management Center. The algorithm inputs the security factor λ and the attribute space U to generate the system public key PSK and the system master key MSK:

$$\text{Setup}(\lambda, U) \longrightarrow (\text{PSK}, \text{MSK}). \quad (1)$$

(2) Key generation: key generation is executed on the Trusted Key Management Center and provides the attribute association key USK for the data requestor based on the system public key PSK, the system master key MSK, and the attribute set A submitted by the data requestor:

$$\text{KeyGen}(\text{PSK}, \text{MSK}, A) \longrightarrow \text{USK}. \quad (2)$$

(3) Plaintext encryption: plaintext encryption is executed by the rail transit data owner to generate the ciphertext CT for attribute encryption by using the system public key PSK, the information to be encrypted T, and the access control structure A_{cp} associated with the access policy:

$$\text{Encrypt}\left(\text{PSK}, T, A_{\text{cp}}\right) \longrightarrow \text{CT}. \quad (3)$$

(4) Ciphertext decryption: decryption is performed by the data requester to obtain the plaintext T based on the system public key PSK, the attribute association key USK, and the attribute-encrypted ciphertext CT:

$$\text{Decrypt}(\text{PSK}, \text{USK}, \text{CT}) \longrightarrow T. \quad (4)$$

3.4. Blockchain-Based Distributed Data-Sharing Solution for Rail Transit. We combine blockchain and IPFS to design a distributed data-sharing scheme. The data are stored in IPFS in a distributed manner, and the data access control function is realized by deploying special functional blockchain smart contracts, which in turn guarantees the absolute control of data holders over the data.

As shown in Figure 2, the rail transit data-sharing platform is composed of two parts: on-chain and off-chain. The on-chain part is mainly a blockchain platform, which is responsible for data-sharing information on-chain storage, data-sharing access control, and on-chain identity information registration update. The off-chain part includes IPFS and trusted third-party key distribution center, which are mainly responsible for rail transit data storage, key distribution, identity registration, and e-verification.

The data-sharing information stored in the upper part of the chain includes information of data owners, information of data visitors, and some operation information of visitors accessing data, which includes reading and downloading of rail transit data. Based on these information, the rail transit data-sharing platform can strictly supervise the data access behavior of data requesters, and the rail transit data will be stored in the IPFS.

The blockchain-based rail transit data-sharing process is divided into three parts as follows:

(1) Rail transit data release: Figure 3 shows the process of publishing rail transit data. The owner of rail transit data needs to join the blockchain and IPFS first. After passing the identity authentication, the data source can be built or hosted. Then, it needs to write the detailed description of the rail transit data and the sharing related protocol to IPFS and publish the file. Then, the name and hash value of rail transit data are written to the blockchain, and after broadcast by the blockchain, the blockchain consensus is completed and synchronized across the network. This is the end of the rail transit data publishing process.

(2) Rail transit data request: Figure 4 shows the request process of rail transit data sharing. The node requesting data first needs to join the blockchain after authentication and then retrieve the required dataset according to the data name and hash value. It also obtains files such as data information and sharing protocols from IPFS. Then, select the eligible files to initiate rail transit data sharing, followed by downloading the relevant files to the local area, and finally, the blockchain performs consensus and stores them in the whole network. All operations during its data-sharing process are recorded.

(3) Rail transit data-sharing authority interaction: Figure 5 shows the interaction process of rail transit data-sharing authority. The owner of the rail transit data needs to review the identity information and request content of the data requestor. If the request does not meet the requirements, it is rejected directly. If it meets, the data access method is encrypted with the public key of the data requestor and written to IPFS according to the access control policy. Then, the data requestor will decrypt the downloaded file with the private key and obtain the access method. After accessing the dataset, the data-sharing interaction is completed and the permission interaction process is finished.

4. Evolutionary-Based Urban Transit Data-Sharing Strategies Design and Optimization

Take rail transit passenger flow data prediction as an example; the realization of passenger flow prediction needs the support of data sharing. By analyzing passenger boarding and alighting information and passenger flow etc., with machine learning methods, the prediction of passenger flow at the next time can be realized, thus helping operators to make reasonable operation plans, effectively alleviating traffic congestion, and improving the operation efficiency of urban rail transit systems. In the process of forecasting, the size of passenger flow data determines the effectiveness of passenger flow forecasting. However, each operator can only

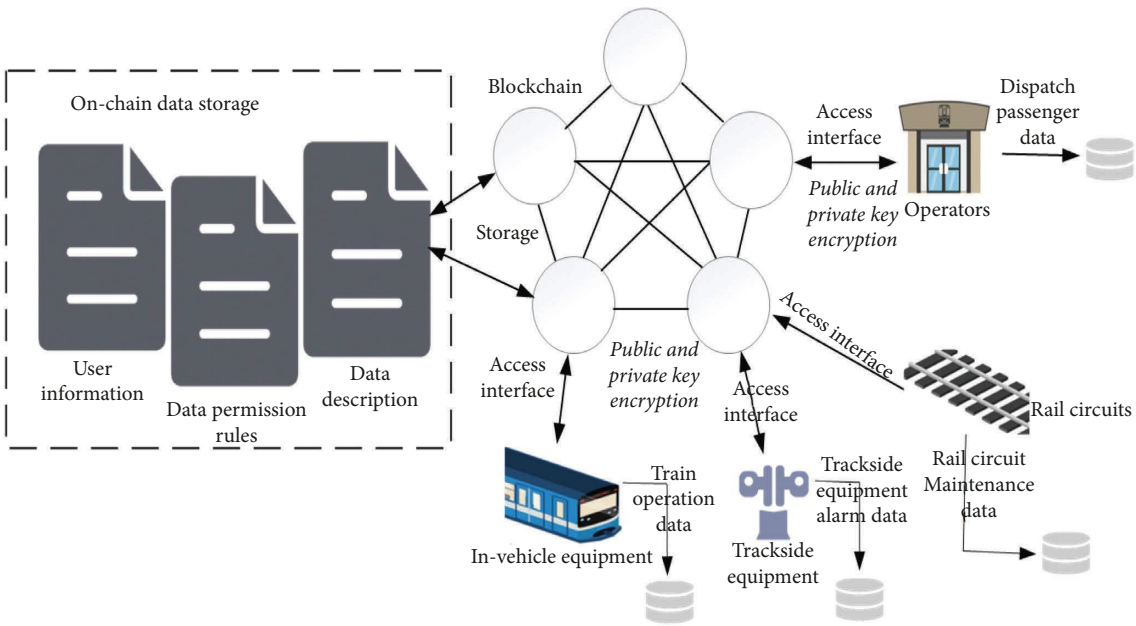

Figure 2: Blockchain-based distributed rail transit data-sharing platform.

get the passenger data of its own operation section, which is not shared among the operators, and the lack of data affects the prediction accuracy of passenger flow. Therefore, we need to design an effective data-sharing incentive mechanism to encourage operators to share data to achieve accurate passenger flow prediction.

Therefore, we create an evolutionary game payoff matrix and use EGT to analyze the evolutionary game process of the rail transit data generation node A and B (i.e., system user A and user B), analyze the final evolutionary direction of the game, and design an effective incentive mechanism to break the data barriers among rail transit operators based on the evolutionary results. Basically, the game is a two-player game where user A and user B generate their own data and share it with each other. After that, the data receiver has to analyze the data and reward the data sharer based on his progress.

4.1. Problem Formulation and Assumptions. In our proposed data-sharing framework based on blockchain, users are playing games with each other most of the time. Accurately, users share their data to get reward from other users of the trading program (aka data requesters), and each user can decide whether to engage in the data sharing or not [28]. Obviously, users' proportion to share data is an ongoing process affected by environment, incentive mechanism, and interactions among users, so users' proportion to share data is an evolutionary process [29]. Therefore, after constructing the EGT model, the influencing factors of the spread of sharing intention among users can be analyzed. The EGI model is based on the following concepts:

(1) Players: we consider the situation where two users play against each other in our proposed model, i.e., user A and user B. The participants are all self-interested, the information of everyone's strategic choices is symmetrical, and decisions are made in order [30].

(2) Strategy space: users can choose from a strategy space of [P, N], where P refers to the participation strategy and N is the opposite [31].

(3) Incentive reward: to increase the proportion of users' sharing data, we assume that there is a mechanism

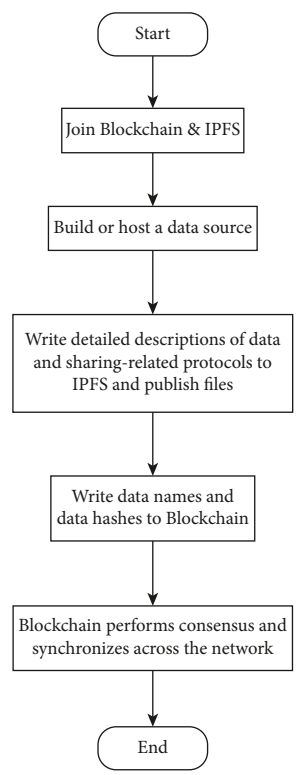

Figure 3: Rail transit data release process.

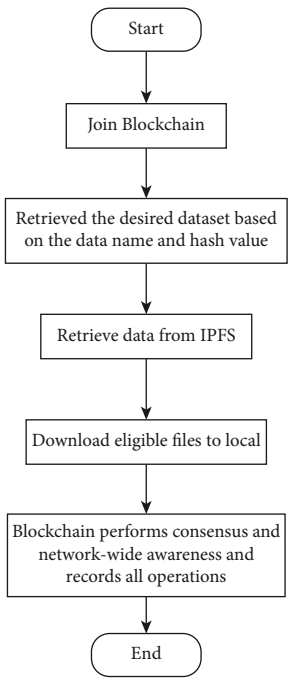

Figure 4: Rail transit data-sharing request process.

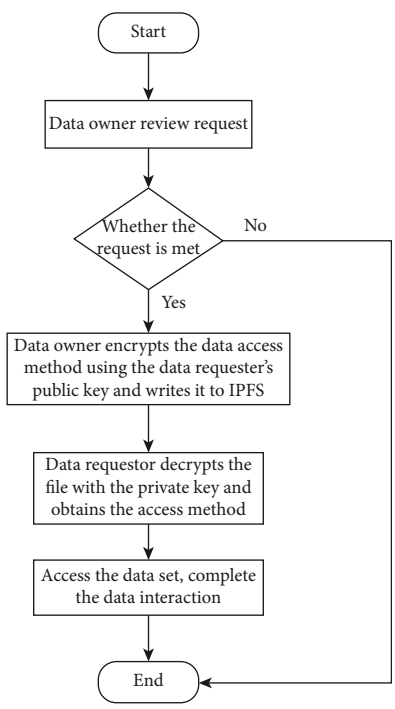

Figure 5: Rail transit data-sharing permission interaction process.

that allows users to obtain a reward R_i for one data sharing.

(4) Shared income magnification: if both parties participate in data sharing, both parties can obtain the data shared by other users and help the other party obtain more benefits. Therefore, we assume that the user's income is multiplied by $\gamma(\gamma > 1)$ times at this time.

(5) Parameters: other parameters and concepts used in the model are listed in Table 1

Based on the above assumptions and defined parameters, we can deduce that there are four combinations of strategies that both users may choose in this model, namely, [P, P], [P, N], [N, N], and [N, P], and the utility matrix of the game is listed in Table 2.

Setting the proportion of data shared by user groups $X(t) = x$, with $x \in [0, 1]$ based on Table 2, we infer the expected income of users who make strategy (P) as

$$I_U(P) = x[\gamma R_s - C_s + R_i] + (1 - x)[R_s - C_s + R_i]. \quad (5)$$

The expected income of users with strategy (U) is

$$I_U(N) = x[R_n - C_n] + (1 - x)[R_n - C_n], \quad (6)$$

and the expected income of total users is

$$I_U = xI_U(P) + (1 - x)I_U(N). \quad (7)$$

4.2. Evolutionary Game-Based Solution Method and Steady State Analysis. According to the Malthusian growth model, the growth rate of the proportion of users' sharing data is positively related to the utility and expected return of the incentive strategy. Hence, according to (1) or (2), the RDE of the proportion of users sharing data (noted later as RDE_x) is expressed as

$$F(x) = \frac{\mathrm{dx}}{\mathrm{dt}} = x(I_U(P) - I_U). \quad (8)$$

Simplify (4) to obtain

$$F(x) = \frac{\mathrm{dx}}{\mathrm{dt}} = x(1 - x)[(x\gamma + 1 - x)R_s + R_i - C_s - R_n + C_n]. \quad (9)$$

Thus, according to (5), we can get three equilibrium points:

$$\begin{aligned} x_1^* &= 0, \\ x_2^* &= 1, \\ x_3^* &= \frac{C_s + R_n - C_n - R_i - R_s}{R_s(\gamma - 1)}. \end{aligned} \quad (10)$$

According to differential equation stability theory, if x^* is a steady state, it must satisfy $F\prime(x^*) < 0$.

Case I: if $R_s + R_i - C_s < R_n - C_n < \gamma R_s + R_i - C_s$ meaning that the income from choosing strategy (N) is higher than the income from choosing strategy (P) when the other party chooses strategy (N) and lower than the income from choosing strategy (P) when the other party also chooses strategy (P), the stability of these three points is analyzed in Table 3. The results show that x_1^* and x_2^* are both evolutionary stable strategies (ESS) [32], which means that achieving a specific ESS depends on the initial proportion of users participating in data sharing. When $0 < x < C_s + R_n - C_n - R_i - R_s/R_s(\gamma - 1)$, ESS tends to be strategy (U),

Table 1: Parameters.

Symbols	Definition
R_s	Rewards from participating in data sharing
C_s	Cost from participating in data sharing
R_n	Rewards from not participating in data sharing
C_n	Cost from not participating in data sharing
R_i	Incentive rewards from participating in data sharing
γ	Scaling parameters for users to gain from shared data

Table 2: Payoff matrix.

User A and User B	Participative	Nonparticipative
Participative	$\gamma R_s - C_s + R_i, \gamma$, $R_s - C_s + R_i$	$R_s - C_s + R_i$, $R_n - C_n$
Nonparticipative	$R_n - C_n$, $R_s - C_s + R_i$	$R_n - C_n$, $R_n - C_n$

and when $C_s + R_n - C_n - R_i - R_s/R_s(\gamma - 1) < x < 1$, ESS tends to be strategy (P) meaning that if the initial percentage of users involved in data sharing is higher than a certain threshold (i.e., $C_s + R_n - C_n - R_i - R_s/R_s(\gamma - 1) < x < 1$), the rest of the users will choose strategy (P) as time goes by. Similarity, if the initial percentage of users involved in data sharing is lower than the threshold, ESS tends to be strategy (N).

Case II: if $R_n - C_n > \gamma R_s + R_i - C_s$ meaning that the income from choosing strategy (N) is higher than the income from both parties choosing strategy (P). The stability of these three points is analyzed in Table 4. The results show that x_1^* is the only ESS, which means that whatever the initial percentage of users involved in data sharing and the users will choose strategy (N). Because, in this case, strategy (N) brings the most income, the initial group adopting strategy (P) can easily be invaded by a small group of groups adopting strategy (N).

Case III: if $R_n - C_n < R_s + R_i - C_s$ meaning that the income from choosing strategy (N) is lower than the income from choosing strategy (P) when the other party chooses strategy (N), the stability of these three points is analyzed in Table 5. The results show that x_2^* is the only ESS, which means that whatever may be the initial percentage of users involved in data sharing, the users will select strategy (P).

Above all, the evolutionary stable strategy trend of EGI incentive model is shown in Figure 6, and the dynamic phases of the evolution of the proportion of users participating in data sharing of all cases are discussed in Section 5.

5. Performance Analysis

5.1. Numerical Analysis. To verify the stable strategy of users participating in data-sharing evolutionary games in the above three cases and show how the strategy stability influenced by certain parameters in the game, we satisfy three different cases by setting different values of R_s, C_s, R_n, C_n, R_i, and γ as shown in Table 6 and use Matlab to simulate the evolution process; the simulation results are shown in Figure 7.

In Figure 7(a), we set two initial proportion of users participating in data sharing to satisfy the first case: one is $x = 0.1$, lower than the threshold x_3^*, and the other is $x = 0.4$, higher than the threshold x_3^*. Hence, when $x = 0.1$, the user group will eventually evolve into a group that chooses strategy (U) in the game, and when $x = 0.4$, it will evolve towards strategy (P) which verifies the theoretical results.

To satisfy the second case, we start with $x = 0.5$ in Figure 7(b). The result shows though most of the initially

Table 3: Stability of equilibrium points (case I).

Equilibrium point	$F'(x^*)$	Stability
x_1^*	−	Stable
x_2^*	−	Stable
x_3^*	+	Unstable

Table 4: Stability of equilibrium points (case II).

Equilibrium point	$F'(x^*)$	Stability
x_1^*	−	Stable
x_2^*	+	Unstable
x_3^*	—	—

Table 5: Stability of equilibrium points (case III).

Equilibrium point	$F'(x^*)$	Stability
x_1^*	+	Unstable
x_2^*	−	Stable
x_3^*	—	—

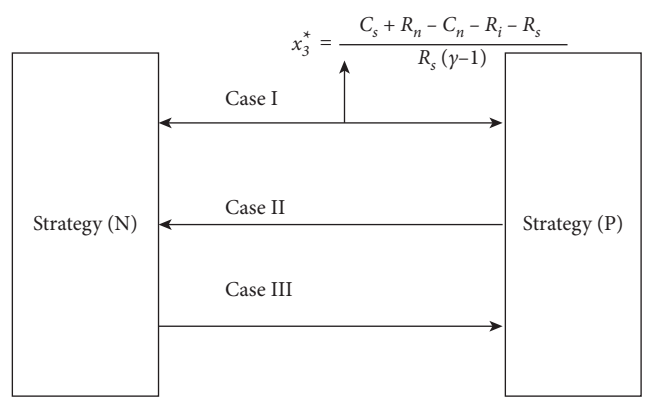

Figure 6: Evolutionary stable strategy trend of the EGI incentive model.

Table 6: Evolutionary game parameter settings.

	Parameter					
Case	R_n	C_n	R_s	C_s	R_i	γ
I	9	4	6	5	3	2
II	16	4	6	5	3	2
III	7	4	6	5	3	2

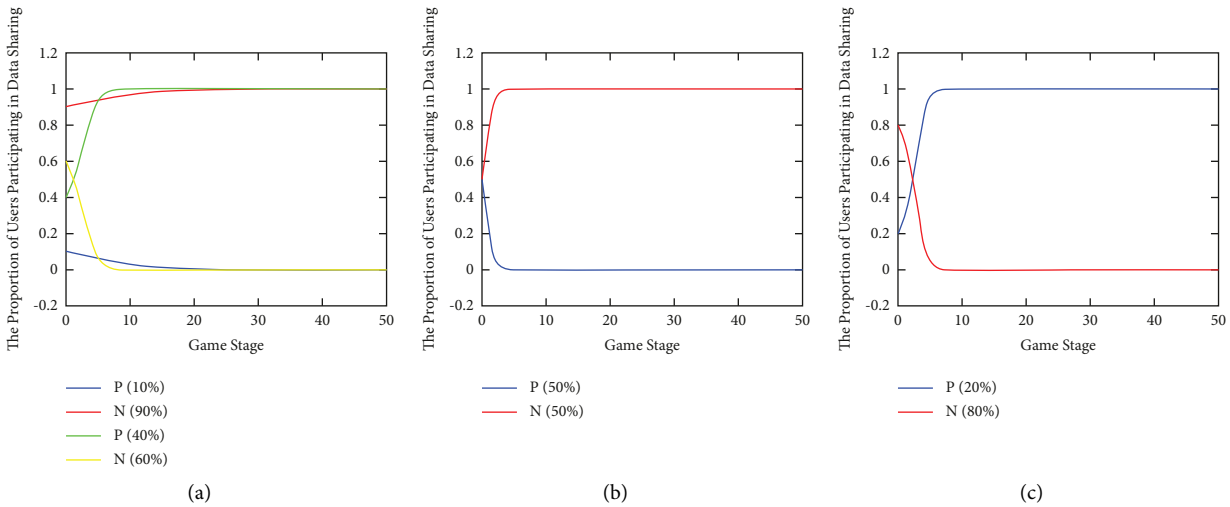

Figure 7: Dynamic stages in the evolution of the percentage of users involved in data sharing. (a) Case I, (b) Case II, and (c) Case III.

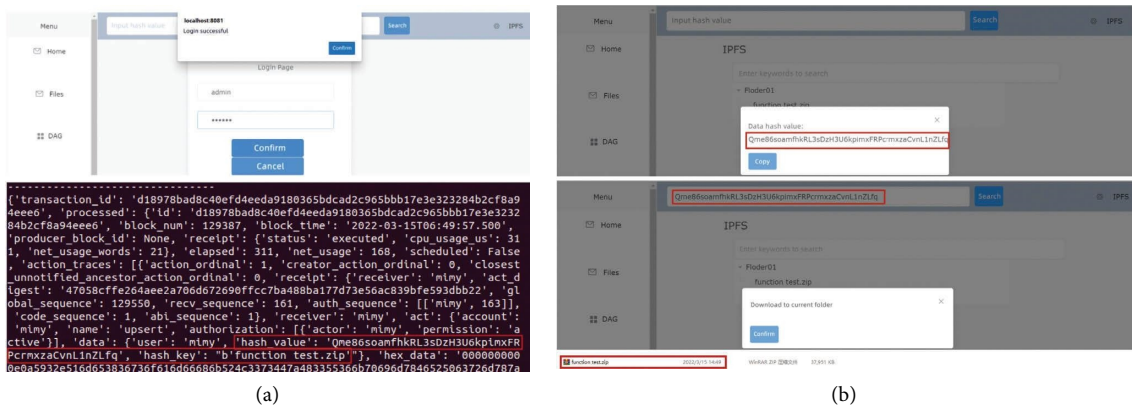

Figure 8: The system functions test. (a) Upload rail transit data. (b) Download rail transit data.

Figure 9: The system performance test.

users choose strategy (P) at first, the game eventually moves towards an nonparticipative group.

Finally, the evolution in the third case is presented in Figure 7(c), even if we only start the game with $x = 0.2$, the game will still evolve towards strategy (P), which matches the above theoretical analysis results [33].

Therefore, to control the final direction of evolution, we only need to set the parameter values to satisfy certain conditions based on the above parameters. That is, in order to encourage data sharing among operators, we can set the parameter values to satisfy Case I so that the final evolutionary trend will move in the direction of strategy (P) and the data barriers will be broken, regardless of the initial decision on the proportion of operators participating in data sharing.

5.2. System Functions and Performance Test. To ensure the system functional integrity and the efficiency of data transmission, we test the system's functions and simulate the data upload process of the data generation node and measure the data upload rate. The system function test results are shown in Figure 8. We implement blockchain-based data upload and download, which means the system has a complete prototype. We also test the real-time rate of rail traffic data upload. Since a large file (for example, a 1G file) will be broken when uploading to IPFS, forming multiple file fragments, each fragment is 256 KB, the uploading process of fragments is performed synchronously, and the storage node will store it according to its want-list table. In the other words, the data storage method of IPFS is that many storage nodes start to store fragments of large data files synchronously. When all fragmented files are stored, the storage work is completed. We measure the upload rate of a single fragment. As shown in Figure 9, the data upload rate reached 50KiB/s, which can meet the daily needs of urban rail transit data generation nodes.

6. Conclusions

In this study, we presented the design of a distributed data-sharing system based on blockchain to provide an efficient and secure data-sharing environment to promote more users to involve in data share. We also utilized EGT to analyze the evolution of user data-sharing behaviour in our designed system. The process of the relevant parameters affecting data-sharing behavior under three cases is studied in detail, and numerical simulation analyses are conducted, which are carried out by controlling the relevant parameters and the initial proportion of users involved in data sharing. We also verified the percentage of users involved in data sharing can be improved by adjusting the incentive parameters. Finally, we conducted functional and performance tests on the designed blockchain-based distributed data-sharing system, and the results showed that the upload rate of a single file fragment of size 256 KB can reach 50KiB/s in this system, and each file is broken into multiple file fragments and uploaded at the same time, and the performance of the system can meet the daily demand of rail transit data generation nodes. It can be seen that this distributed file transfer system provides a solution to enhance the data-sharing rate of rail transit.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported by Beijing Natural Science Foundation (L201002), the Natural Science Foundation of China under Grants (61973026), Beijing Municipal Education Commission Funding (I20H100010, I19H100010), in part by the Beijing Jiaotong University Project under Grant (RCS2021ZZ005), and Fundamental Research Funds for the Central Universities (2021CZ107).

References

[1] R. Akkaoui, X. Hei, and W. Cheng, "An evolutionary game-theoretic trust study of a blockchain-based personal health data sharing framework," in *Proceedings of the 2020 Information Communication Technologies Conference (ICTC)*, pp. 277–281, Nanjing, China, May 2020.

[2] Y. H. Shan, L. I. Zhong-Fu, and S. O. Management, "Evolutionary game analysis of knowledge-sharing mechanism of construction supply chain towards construction industrialization," *Journal of Engineering Management*, vol. 29, 2015.

[3] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: a decentralized, privacy-preserving and secure design," in *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, December 2018.

[4] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: using blockchain for medical data access and permission management," in *Proceedings of the International Conference on Open Big Data*, Vienna, Austria, August 2016.

[6] L. Yan, "Study on the System Structure and Construction Thinking of Big Data Public Platform," *Library Theory and Practice*, 2017.

[7] J.-B. Poline, J. L. Breeze, S. Ghosh et al., "Data sharing in neuroimaging research," *Frontiers in Neuroinformatics*, vol. 6, p. 9, 2012.

[8] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 1–2700, 2022.

[9] J. Wang, M. Chen, G. Lü et al., "A data sharing method in the open web environment: data sharing in hydrology," *Journal of Hydrology*, vol. 587, Article ID 124973, 2020.

[10] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings of the 2015 IEEE Security and Privacy Workshops*, pp. 180–184, IEEE, San Jose, CA, USA, May 2015.

[11] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, pp. 839–858, IEEE, San Jose, CA, USA, May 2016.

[12] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-Of-Things Design and Implementation (IoTDI)*, pp. 173–178, IEEE, Pittsburgh, PA, USA, April 2017.

[13] P. Linder, "Decryption Contract Enforcement Tool (Decent): A Practical Alternative to Government Decryption Backdoors," *Cryptology ePrint Archive*, 2016.

[14] N. Kostić and X. Tang, "The Future of Audit: Examining the Opportunities and Challenges Stemming from the Use of Big Data Analytics and Blockchain Technology in Audit Practice," *Accounting and Finance*, 2017.

[15] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: a global naming and storage system secured by blockchains," in *Proceedings of the 2016 USENIX Annual Technical Conference (USENIX ATC 16)*, pp. 181–194, Denver, CO, Colorado, April 2016.

[16] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for iot data trusted exchange based-on blockchain," in *Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1180–1184, IEEE, Chengdu, China, December 2017.

[17] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "Controlchain: blockchain as a central enabler for access control authorizations in the iot," in *Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6, IEEE, Singapore, December 2017.

[18] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *IFIP International Conference on Distributed Applications and Interoperable Systems*, pp. 206–220, Springer, Berlin, Germany, 2017.

[19] X. Xu, C. Pautasso, L. Zhu et al., "The blockchain as a software connector," in *Proceedings of the 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, pp. 182–191, IEEE, Venice, Italy, April 2016.

[20] R. Krawiec, D. Housman, M. White et al., "Blockchain: opportunities for health care," *Proceedings of the NIST Workshop Blockchain Healthcare*, pp. 1–16, 2016.

[21] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2739–2750, 2019.

[22] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA annual symposium proceedings*, vol. 2017, p. 650, American Medical Informatics Association, 2017.

[23] T.-T. Kuo and L. Ohno-Machado, *Modelchain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks*, 2018, https://arxiv.org/abs/1802.01746.

[24] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for ai-powered network operations," *Journal of Communications and Information Networks*, vol. 3, no. 3, pp. 1–8, 2018.

[25] L. Liu, J. Feng, Q. Pei et al., "Blockchain-enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor–critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.

[26] L. Zhu, H. Liang, H. Wang, B. Ning, and T. Tang, "Joint security and train control design in blockchain-empowered cbtc system," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8119–8129, 2022.

[27] Bitcoin, *A Peer-To-Peer Electronic Cash System*, Decentralized Business Review, 2008.

[28] H. Abbass, G. Greenwood, and E. Petraki, "The n -Player Trust Game and its Replicator Dynamics," *IEEE Transactions on Evolutionary Computation*, vol. 20, no. 3, pp. 470–474, 2016.

[29] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communication Letters*, vol. 99, 2017.

[30] C. Hao, Q. Du, Y. Huang, L. Shao, and Y. Yan, "Evolutionary game analysis on knowledge-sharing behavior in the construction supply chain," *Sustainability*, vol. 11, no. 19, p. 5319, 2019.

[31] C. Lei, D. H. Ma, and H. Q. Zhang, "Optimal strategy selection for moving target defense based on Markov game," *IEEE Access*, vol. 5, no. 99, pp. 156–169, 2017.

[32] J. Li and G. Kendall, "The effect of memory size on the evolutionary stability of strategies in iterated prisoner's dilemma," *IEEE Transactions on Evolutionary Computation*, vol. 18, no. 6, pp. 819–826, 2014.

[33] A. Ghoneim, G. W. Greenwood, and H. Abbass, "Distributing Cognitive Resources in One-Against-many Strategy Games," *in Evolutionary Computation*, 2016.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 1164125, 11 pages
https://doi.org/10.1155/2022/1164125

Research Article

Detecting Fake Reviews with Generative Adversarial Networks for Mobile Social Networks

Zheng Qu,[1] **Qingyao Jia**,[2] **Chen Lyu**,[1] **Jia Liu**,[3] **Xiaoying Liu**,[4] **and Kechen Zheng**[4]

[1]*School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai 200433, China*
[2]*Hwabao WP Fund Management Co., Ltd., Shanghai 200120, China*
[3]*Center for Strategic Cyber Resilience Research and Development, National Institute of Informatics, Tokyo 101-8430, Japan*
[4]*School of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, Zhejiang 310023, China*

Correspondence should be addressed to Chen Lyu; lyu.chen@sufe.edu.cn

Received 8 September 2022; Accepted 6 October 2022; Published 10 November 2022

Academic Editor: Jianbo Du

With the growth of mobile social networks (MSNs), crowdsourced information could be used for recommendation to mobile users. However, it is quite vulnerable to Sybil attacks, where attackers post fake information or reviews to mislead users for business benefits. To address this problem, existing detection models mainly use graph-based techniques or extract features of users. However, these approaches either rely on strong assumptions or lack generalization. Therefore, we propose a novel Sybil detection model based on generative adversarial networks (GANs), which contains a feature extractor, a domain classifier, and a Sybil detector. First, the feature extractor is proposed to identify the rich information in the review text with the neural network model of TextCNN. Second, the domain classifier is implemented by a neural network discriminator and is able to extract common features. Third, the Sybil detector is utilized to discriminate the fake review. Finally, the minimax game between the domain classifier and Sybil detector forms a GAN and enhances the overall generalization ability of the model. Extensive experiments show that our model has a high detection accuracy against Sybil attacks.

1. Introduction

A growing number of mobile social networks (MSNs) in recent years have focused on the contents of social activities, such as eating, traveling, and shopping. For a specific activity or product, each user can give a review or rate it. With the Internet and mobile social platform, this information can be posted in real time. If other users are interested in it, they may collect information based on the reviews provided by the platform and adjust their consumption behavior according to the rating from other users. With the commercialization of MSNs, they have become popular platforms to share information and recommend products. Users can easily post reviews about merchants and obtain other people's reviews on the platforms.

Despite the convenience offered by MSNs, product reviews face severe security threats on the platforms such as Yelp and Dianping. On the one hand, users' reviews are usually posted individually and anonymously. It is difficult to access any information about users in the real world, making it hard to authenticate them. On the other hand, users are hard to verify the validity of a review based on the content of the review alone. Users post reviews on social networks based on their personal consumption experience, and MSNs make personalized recommendations based on the user's situation as well. Actually, merchants with high scores are more likely to capture customers, which may attract merchants to maliciously post fake reviews to improve their scores. This makes users' reviews become the targets of Sybil attacks, which is a major concern for many operators of MSNs.

The concept of Sybil attack was first applied to computer security which creates a large number of false identities (i.e., user accounts) and has a significant security threat to a system. Sybil attackers often manipulate social media through misinformation, defamation, spam, malware, or even just unrelated noise [1]. According to Yelp's 2021 Trust

and Safety Report, Yelp generated more than 19.6 million reviews in 2021, of which only about 71% were recognized as recommended reviews to be displayed by the platform. About 29% of reviews were considered non-compliant reviews, which have various issues including possible conflicts of interest, false, useless, or unreliable. Therefore, a reliable Sybil attack detection scheme is essential for the MSNs.

Unlike traditional Sybil attacks launched by fake accounts in online social networks, Sybil attacks in MSNs deceive customers by recruiting real users to generate fake content, which makes many existing Sybil detection approaches based on user behaviors fail (e.g., [2, 3]). Figure 1 illustrates a typical Sybil attack in Dianping. For a Sybil attack, an agent often hires real users and includes relevant requirements in the task posting, which specify the object and aspect of an attack. Compared to traditional online social networks (e.g., Twitter or Weibo), MSNs also greatly diminish the impact of user relationships as their users are not closely connected. This is because the main purpose of users is to learn about a product or merchant through other users' reviews, rather than communicating directly. Therefore, this feature makes previous graph-based approaches [4–8] ineffective. Other studies [9–11] have demonstrated that text features could provide good results for fake news detection. However, unlike news, features extracted from reviews are relatively scarce and variable, leading to these approaches being less efficient. In addition, reviews in MSNs are related to the product category, making the text features highly correlated with it. Hence, they lack the generalizability of detection of Sybil attacks.

In this work, we propose a Sybil attack detection model based on generative adversarial networks (GANs) to improve the accuracy and generalization of MSNs. Inspired by the idea of GANs, our model has three significant components: a feature extractor, a domain classifier, and a Sybil detector. First, to construct the feature extractor, we make use of the neural network model of text convolutional neural network (TextCNN) to extract text features of reviews, which would be input to the Sybil detector and domain classifier. Second, we make use of a neural network discriminator to design the domain classifier. The discrimination loss is set to be maximized, and therefore the learned features are common features unrelated to the product category. Third, based on the extracted text features, we design the Sybil detector with a fully connected layer to detect the fake reviews of Sybil attacks. Finally, we constitute a GAN using the minimax game between the domain classifier and the Sybil detector. Based on the real data crawled from Dianping, we validate our model and compare it with 9 state-of-the-art approaches. The extensive experiments show that our model has the best performance against Sybil attacks.

As far as we know, our model is the first Sybil detection model with GANs in MSNs. Our contribution can be summarized as follows:

(i) We design a Sybil detection model based on GANs to provide the generalizability of the model for MSNs, which includes a feature extractor, a domain classifier, and a Sybil detector.

(ii) We make use of the neural network model of TextCNN to construct the feature extractor and extract the text features of reviews.

(iii) We introduce the domain classifier with a neural network discriminator, which is able to learn common features.

(iv) We propose a GAN using the minimax game between the domain classifier and the Sybil detector. Through extensive experiments on Dianping, our GAN model effectively improves the detection accuracy of Sybil attacks.

The organization of the rest of the paper is as follows. We present the related work in Section 2. The description of data crawling, preprocessing, and annotation is given in Section 3. In Section 4, we present the construction of our model. Extensive experiments are conducted and analyzed in Section 5. At last, we conclude our work in Section 6.

2. Related Work

We list the literature related to our study and classify them into two categories based on their research focus. The first concentrates on the detection of Sybil attacks, and the second targets GANs.

2.1. Sybil Attacker Detection. Most previous research has focused on detecting Sybil attackers in online social networks (OSNs), such as fake accounts and spammers on Twitter. They mainly construct a graph of user relationships in the social networks using graph-based techniques. In the graph, nodes of the graph represent users and edges of the graph represent relationships.

Wei et al. [4] relied on social network graphs and proposed a mechanism of Sybil defense, which uses the metric to measure the relationship of users and thus decrease the number of edges of Sybil attacks. Effendy and Yap [5] made use of strongly connected graphs and strengthened the defense by decreasing the number of edges of Sybil attackers. Experimental results show that the defensibility of their method can be recovered once suspicious edges are removed. Furutani et al. [6] gave an explanation about the task of Sybil detection in terms of signal processing of graphs and proposed a general framework to design an approach for Sybil detection with both belief propagation and random wandering. Zhang et al. [8] improved the detection rate of Sybil attacks by integrating local structural similarity matching, regularization algorithms, and graph pruning in the graph networks. To detect Sybil attacks, Xue et al. [7] proposed a combination of graph edges and user feedback information for social networks. All these methods making use of graph models rely on the strong assumption that users are closely connected to each other, which only applies to OSNs [12]. However, the relationship between users is quite sparse for recommendations in the MSNs, since most users are not connected to others. Hence, building such an effective graph model is impossible for users in MSNs.

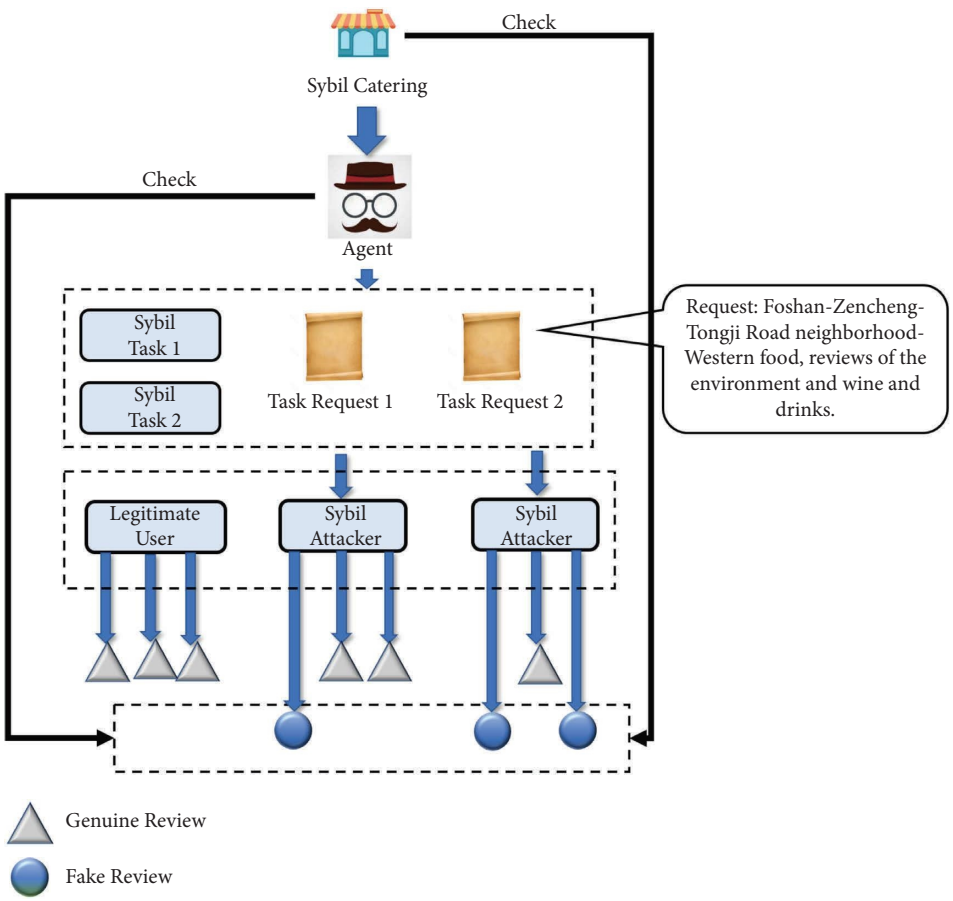

Figure 1: The flow of a Sybil attack.

Another important approach for Sybil detection is to deploy feature extraction techniques. Rahman et al. [13] took the impact of Sybil attackers into account and then made use of the parameters of user impact weights for Sybil detection. Egele et al. [14] proposed a model to identify anomalous users during a short time which is able to detect account theft. These two approaches mainly extract user features from textual content for Sybil detection. For OSNs, Ramachandran et al. [3] extracted user behavior features (e.g., replies) and network-based features (e.g., IP addresses) and then proposed a spam detection system. In Twitter, Song et al. [2] designed a method for fake review detection utilizing the feature of retweeting. In MSNs, Zhang et al. [15] used behavioral features of users and location-based features to detect Sybil attacks. Lyu et al. [16] introduced spatial-temporal features and users' preference features and combined them with traditional features to improve the detection accuracy of Sybil attackers.

All these methods based on user features have two drawbacks for detecting Sybil attacks in MSNs. On the one hand, since Sybil attackers often try to imitate the behaviors of real users in MSNs, these methods cannot distinguish real users and Sybil attackers by only extracting user features. On the other hand, they lack generalizability due to the natural limit of feature engineering. In this work, we make use of a neural network model to construct a detection model based on GANs, aiming to improve the accuracy and generalization against Sybil attacks.

2.2. Generative Adversarial Networks. Our work is inspired by the idea of GANs [17]. Existing GANs usually generate images that match the observed samples by means of a framework of minimax game.

Makhzani et al. [18] proposed a probabilistic self-encoder that deploys GANs to perform variational inference by matching the posterior of the self-encoder with an arbitrary prior distribution to ensure the distribution of the generated samples. Lipton and Tripathi [19] made use of a simple, gradient-based timely cropping technique that combines with GANs to transform potential vectors into visually plausible images. The robustness of their method was verified through experiments on unseen images. Ganin and Lempitsky [20] proposed a GAN-based deep learning framework in the absence of task-specific labeled data. They used few standard layers and a simple new gradient inversion layer for data augmentation to obtain better performance for small samples.

Pu et al. [21] designed a new GAN for joint distribution matching. Unlike other methods that only learn conditional distributions, their proposed model is able to learn the joint distribution of multiple random variables (domains), which establishes minimax games between event discriminators

and multimodal feature extractors. In particular, since the multimodal feature extractor is forced to learn a static representation of events in order to deceive the discriminator, it eliminates the tight dependence on specific events in the collected dataset and achieves a better generalization capability on unseen events. Since GANs perform outstandingly well for image and text processing, we explore the core idea of GANs and leverage it for detecting Sybil attacks in the MSNs.

3. Dataset

3.1. Dataset Description. Dianping is the largest and most popular mobile social network for recommendation in China. According to the official data, Dianping has over 250 million active users and over 150 million reviews per month in China. When a user visits Dianping, it suggests a list of local merchants (e.g., restaurants) based on keywords entered by the user or his current geographic location, which is usually sorted by the merchant's rating. According to Dianping's rules, the star rating of a merchant is a combination of the overall rating of the site's users and is automatically updated by the system based on a scientific formula without any human intervention. Users score the merchant's taste, environment, and service according to criteria ranging from one star to five stars. The system averages all users' scores and then adjusts them according to several predetermined indicators (including the number of reviews, review time, member/merchant's reputation, and so on).

A merchant with a large number of positive reviews on Dianping is a valuable advertisement, since a top-ranked merchant on the praise list tends to attract more users to visit that merchant. As a result, the platform of Dianping has been under constant threat of Sybil attacks, and both the number of positive reviews and ratings are often purposefully manipulated by Sybil attackers. Dianping has established its own review filtering mechanism. When we crawled the data from Dianping, we found that users' reviews are divided into normal reviews and hidden reviews. The hidden reviews are not shown on the default store page or user page, but we can still obtain them using a crawler. Reasons for becoming a hidden review may include that the review lacks sufficient informativeness (default positive reviews or reviews are too short) or that the platform believes the review may be a suspicious review posted by a Sybil attacker. However, the details of Dianping's review filtering algorithm are not available to the public. Moreover, despite the platform's filtering algorithm, fake reviews with commercial fraudulent nature are not completely eliminated.

3.2. Dataset Annotation. In this work, our target is to build a Sybil attack detection model for the review/comment data from Dianping. We crawl the data related to Dianping and acquire the data in the following steps. First, we manually select 12 merchants that have been officially confirmed to have Sybil attacks and crawl the reviews posted under these merchants. Second, based on the list of users in the reviews, we crawl out the personal information of these users and all the reviews they have posted. Finally, we collect a total of 918,373 user reviews.

For the hidden comments, we hire five undergraduate students as annotators to flag Sybil or real but low-quality comments. The annotators were also given full freedom to make use of any relevant information or their own intuition. In terms of some controversial cases, we deployed voting to determine the final outcome. Therefore, a review is marked as Sybil when and only when the results of five votes are SSSLL, SSSSL, or SSSSS, while S stands for Sybil and L stands for the legitimate review that contains low information or invalid positive reviews. The average annotation consistency based on Cohen κ is 0.74, which indicates the consistency property of annotation [22].

4. Our Methodology

In this section, we first introduce the three components of the model proposed in this paper: a feature extractor, a domain classifier, and a Sybil discriminator. Then, we describe how to integrate these three components to establish a generalized learning representation model. The flowchart of our model is shown in Figure 2.

4.1. Feature Extractor. For the Sybil attack in MSNs, we first choose a text feature extractor to extract the text features. Unlike common fake reviews, Sybil attacks are organized. Some Sybil attackers often give verbal hints to show the advantages of products or services, and these reviews are different for various types of products and services. Hence, we choose a text feature extractor to identify the rich information in the review text. Our feature extractor makes use of a convolutional neural network (CNN) as the main feature input module, which was first proposed due to the need for work on images and has been widely used in areas such as image processing [23, 24]. In the year of 2014, Zhang and Wallace [25] first proposed using CNNs to implement sentence classification. The initial TextCNN network has only one convolutional layer and one maximum pooling layer, and the output is connected to softmax for multiple classifications. The general structure diagram of TextCNN is illustrated in Figure 3. In this work, we capture text features of different granularity by adjusting the size of the convolutional window.

In terms of text feature extraction, we first preprocess the raw text of the reviews. We remove non-Chinese and unrecognizable reviews (e.g., text containing only emojis and special symbols) because these samples play no role in model training. We then eliminated information such as punctuation marks or emoticons in the sentences and split the review text using jieba. Jieba is a Python-based Chinese splitting component that can be used for word segmentation, lexical annotation, and keyword extraction. After preprocessing, we remove useless information such as conjunctions in the splitting result according to jieba and finally repatch the text at the end of the splitting to get the split words.

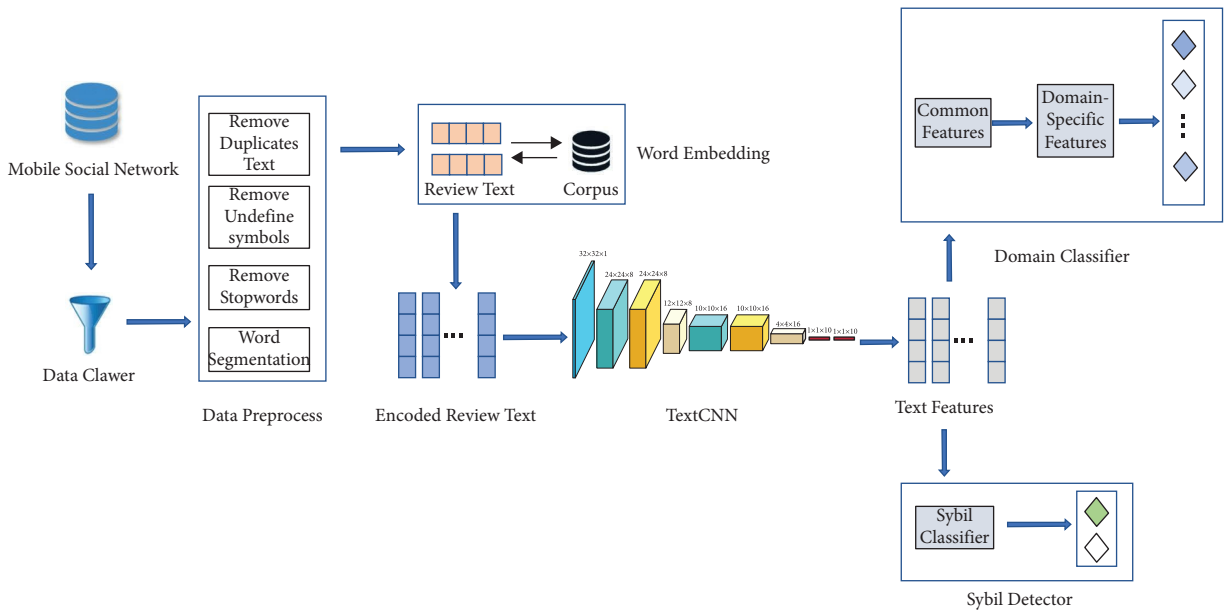

Figure 2: The flowchart of our model.

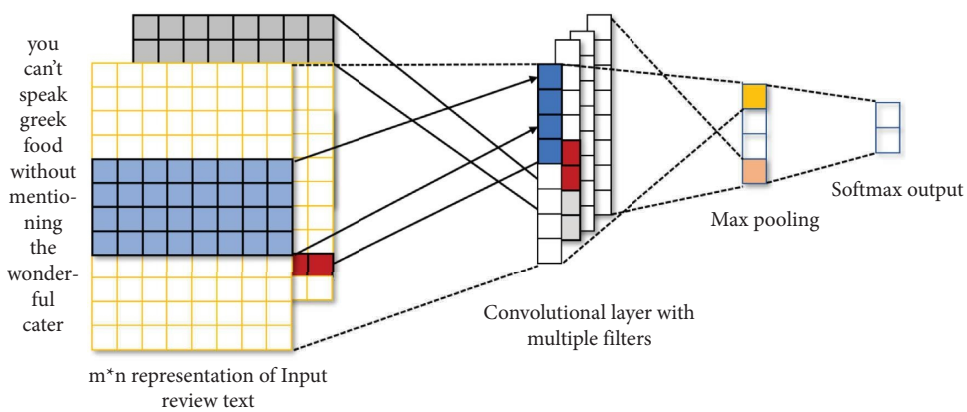

Figure 3: The structure of TextCNN.

Subsequently, we use word2vec to encode the processed text. Previous studies [26, 27] have shown that using a word embedding model can improve the performance of convolutional neural networks to a greater extent than the TextCNN structure adaptation. To obtain the word vector encoding, we choose a pretrained word embedding model that generates a 32-dimensional word vector corresponding to a word. The pretrained model is constructed by skip-gram through an existing lexicon. Compared to large-scale pretrained language models, the word embedding model has lower dimensions and is more suitable for convolutional neural networks. As a result, each word is encoded as a vector. For a given text $D_i$containing the sentence S_j, $S_j = \{w_1, w_2, \ldots, w_{n_j}\}$, when all words w are in the dictionary of the word embedding model, we give the representation of the sentence:

$$V_{S_j} = \text{concate}\left(V_{w_1}, V_{w_2}, \ldots, V_{w_{n_j}}\right), \tag{1}$$

where concate means concatenation of vectors. Similarly, the word embedding of the comment text D_i is represented as

$$V_{D_i} = \text{concate}\left(V_{S_1}, V_{S_2}, \ldots, V_{S_{m_i}}\right). \tag{2}$$

Since the vast majority of the text in the review is within 100 characters in length, we do not consider the long-term dependency between sentences. After getting the input text embedded, the convolution filter of window size z outputs the filtered word vectors based on the input vectors. For word w_k, the output vector after convolution is

$$\text{cov}_z\left(w_k\right) = \text{Relu}\left(W_c \cdot V_{\left[w_{k-\frac{z}{2}}: w_{k+\frac{z}{2}}\right]}\right), \tag{3}$$

$$\text{Relu} = \max\left(0, x\right), \tag{4}$$

where W_c is the weight of the filter and *Relu* is the activation function. The filter converts all words of sentence S_j to a feature vector:

$$cov_z(S_j) = \left[\mathrm{cov}_z(w_1), \ldots, \mathrm{cov}_z\left(w_{n_j-z+1}\right)\right]. \quad (5)$$

We then use maxpooling to extract the maximum value of the features. Maxpooling can reduce the number of model parameters and help to reduce the problem of model overfitting. After the pooling operation, the 2-D or 1-D array is often converted into a single value. For the subsequent convolution layer or fully connected hidden layer, the number of parameters of a single filter or the number of neurons in the hidden layer is reduced. The variable length of inputs can be collapsed into fixed-length inputs. The model of CNN often ends up with a fully connected layer, and its number of neurons needs to be fixed in advance. The text features after the maxpooling operation are denoted as R_f. A fully connected layer is used to obtain the final text features: $F_f(W_f \cdot R_f)$, where W_f is the weight matrix of the fully connected layer.

We denote the text feature extractor as $F_f(R_f; \theta_f)$, where θ_f denotes the parameter to be learned. The output of the feature extractor is used as the input features for the subsequent generation of the adversarial model.

4.2. Domain Classifier. The main purpose of the domain classifier is to learn the category to which a review belongs. During the data processing, we classify review data into K categories, and there are some differences in the text corresponding to different products. The domain classifier determines the category to which the reviews belong by dealing with the output of the feature extractor. In our task, we want to identify fake reviews into different domains by text, which is also able to extract Sybil text features with commonality.

The domain classifier G_d consists of a neural network discriminator with a network structure consisting of a three-layer fully connected neural network and using Relu as the activation function. We give the loss function of the domain classifier as follows:

$$L_d(\theta_f, \theta_d) = \sum_{k=1}^{K} \log\left(G_d\left(F_f\left(R_f; \theta_f\right)\right); \theta_d\right). \quad (6)$$

We could learn the parameter of loss function of domain classifier θ_d by

$$\left(\hat{\theta}_f, \hat{\theta}_d\right) = \arg\max_{\theta_f, \theta_d} L_d(\theta_f, \theta_d), \quad (7)$$

where the loss L_d is calculated by the cross-entropy function. The loss is used to estimate the variability of the different domain distributions. When the loss is large, the difference between reviews' domain distributions is small and the learned features are approximated. This means that the common features of all domain texts are extracted. Therefore, in our model, we prefer the domain loss function to be as large as possible, that is, to maximize the discriminative loss $L_d(\theta_f, \theta_d)$ by finding the optimal parameter θ_f. With this condition, the Sybil classifier of text can find all the Sybil reviews as possible.

4.3. Sybil Detector. In this part, we introduce the Sybil detector, which uses softmax to deploy a fully connected layer to determine whether a review is a Sybil review or not. Our detector is based on the text features extracted from the feature extractor F_f. We denote the Sybil detector as $G_s(F_f; \theta_s)$, where θ_s denotes all parameters included in the detector. Given a review D_i, the probability that this review belongs to Sybil reviews is $P_s(D_i)$:

$$P_s(D_i) = G_s\left(F_f\left(R_f; \theta_f\right); \theta_s\right). \quad (8)$$

We use cross-entropy to calculate the loss of the model:

$$L_s(\theta_f, \theta_s) = \sum_{i=1}^{N} \left[y \log\left(P_s(D_i)\right) + (1-y)\log\left(1 - P_s(D_i)\right)\right], \quad (9)$$

where L_s donates the loss of Sybil detector and N donates the total number of reviews. For a single Sybil review detector, we only minimize the loss function by finding the optimal parameter θ_s:

$$\left(\hat{\theta}_f, \hat{\theta}_s\right) = \mathrm{argmin}_{\theta_f, \theta_s} L_s(\theta_f, \theta_s). \quad (10)$$

The minimization loss can capture class-specific-based representations. However, such features lack generalization. Therefore, we need a generalized learning representation model that captures common features across categories.

4.4. Model Combination Optimization. To establish the generalized learning model, we need to remove the uniqueness of each domain feature. This is completed by measuring the variability of feature representations across domains and removing them to capture feature representations across domains. Therefore, it leads to a minimal and maximal game between the domain classifier and the Sybil detector. On the one hand, the domain classifier tries to trick the detector to maximize the discriminative loss. On the other hand, the Sybil detector aims to discover event-specific information contained in the feature representation to identify the Sybil review. Hence, we construct our model with GANs using the minimax game [28–30]. The overall loss of these two classifiers is expressed as

$$L_{\mathrm{all}}(\theta_f, \theta_d, \theta_s) = L_d(\theta_f, \theta_d) - \lambda L_s(\theta_f, \theta_s), \quad (11)$$

where λ is a parameter that regulates the importance of two classification tasks. Larger λ indicates a higher importance of the domain classification task, and smaller λ indicates a higher importance of the Sybil review detection task in a specific domain. In the experimental part, we investigate the optimal value of λ. For the minimax game, the parameter set we seek is the saddle point of the final objective function:

$$\left(\hat{\theta}_f, \hat{\theta}_d, \hat{\theta}_s\right) = \operatorname{argmin}_{\theta_f, \theta_d, \theta_s} L_{\text{all}}\left(\theta_f, \theta_d, \theta_s\right). \tag{12}$$

We make use of stochastic gradient descent to find the saddle point. We fix the learning rate r and update the loss in each step:

$$\begin{aligned} \theta_f &:= \theta_f - r\left(\frac{\partial L_d}{\partial \theta_f} - \lambda \frac{\partial L_s}{\partial \theta_f}\right), \\ \theta_d &:= \theta_d - r\frac{\partial L_d}{\partial \theta_d}, \\ \theta_s &:= \theta_s - r\frac{\partial L_s}{\partial \theta_s}. \end{aligned} \tag{13}$$

In the experimental section, we compare our model with other approaches and also discuss the effect of the learning rate and the optimization on our model.

5. Experiments

In this section, we separate the data for training and testing and set up evaluation for our model. First, the raw data are analyzed and the distribution of length of reviews is illustrated. Second, a series of basic methods are presented for comparative evaluation. Third, a large number of experiments are done and the performance evaluation of our Sybil detector is shown in detail. Fourth, an ablation study is performed to demonstrate the validity of our model. Finally, we validate our model on different parameters. Our model is evaluated on a server with Intel CPU Xeon W-2123 3.9 GHz and 64G RAM. The GPU of the server is NVIDIA Tesla v100 with CUDA version 10.2. Our model is implemented by Python 3.7, with PyTorch 1.10.0.

5.1. Data Analysis. We analyze the distribution of length of reviews, and the results are shown in Figure 4. The text length analyzed here is the length of the raw review text, which contains emotions and punctuation marks. Hence, the length will be greatly reduced after preprocessing. We choose a criterion of every 30 words and divide the text length into 10 levels. It can be found that more than 1/4 of the comments have no more than 30 words. At the same time, nearly half of the comments are less than 60 words in length, while comments longer than 120 words only account for 30% of the total.

We also count the length distribution of text after symbol removal, since these symbols have no meaning in feature learning of text. The results are shown in Figure 5. More than 30% of valid characters are less than 30 characters in length. The proportion of less than 60 words is more than 50%, and the effective comments longer than 120 words only account for 1/4. By comparing before and after symbol cleaning, we demonstrate the previous hypothesis that text lengths are generally shorter in MSNs. Useless symbols account for a large proportion and are not suitable for general detection models of long text.

In order to reduce the impact of distribution of review length and then reduce the training cost of the model, we choose reviews with higher quality (longer length and relatively obvious features) to form our dataset.

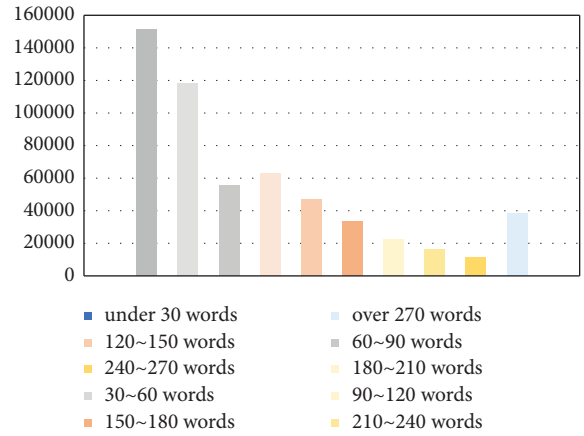

Figure 4: The distribution of length of original review data.

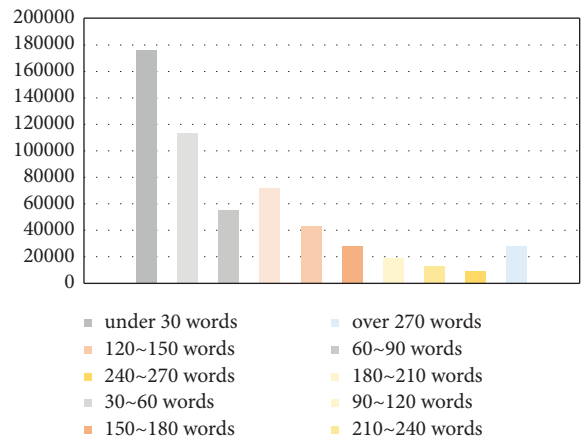

Figure 5: The distribution of length of processed review data.

5.2. Baseline Methods. Benchmark 1 (Classical Machine Learning Model). In the experiment, we select some classical models that are widely used for text classification. To get the best results, we also choose the optimal parameters for each of the models as much as possible.

We select tree-based models, including random forest (with the number of estimators as 20 and max depth as 5), XGBoost (with the learning rate of 0.05 and max depth as 4), and AdaBoost (with the number of estimators as 200, learning rate as 0.05, and estimators as CART decision tree). The input of all these models contains all the text features we extracted.

We choose the logistic regression (with Lasso) as a model for comparison. We also compare our model with SVM (with RBF kernel and penalty parameter as 1) and KNN (with Euclidean distance).

Benchmark 2 (Relevant Model). We also choose another three detection schemes for comparison as they all are deployed in MSNs. The traditional feature model (TFM) makes use of statistical features of users and text features for Sybil detection. Since the feature dimension is low, we use

SVM as the classifier. Zhang et al. [31] utilized both location-based features and traditional features of users to detect Sybil attacks in Dianping. Lyu et al. [16] made use of location-based features, users' preference features, and spatial-temporal features for fake review detection in Dianping.

To evaluate the performance of these models, we will use the following metrics: precision, recall, F1-score, and AUC (area under the ROC curve), which are commonly used in the classification system.

5.3. Model Evaluation. In the experiments, we make the following setups. For the feature extractor, we set the dimension of word embedding k as 32 and the number of filters as 20. In terms of the model of TextCNN, we set the window size of filters from 1 to 5. The hidden size of the fully connected layer in the feature extractor is set to 32. For the Sybil detector, the hidden size of the fully connected layer is set to 64. The domain classifier consists of two fully connected layers. The hidden size of the first layer is set to 64, and the hidden size of the second layer is 32. For all baselines and our proposed model, we use a batch size of 100 in the training phase. The epochs are set to 100, and the learning rate is set to $5e-4$.

We compare our scheme with various baseline methods and give the results in Table 1. For different machine learning models, we choose different methods of text encoding based on the dimension of the input features, since the input dimension will largely affect the performance of the model. For example, in terms of tree-based models, we choose word2vec + TextCNN as the method of text encoding. By comparing different machine learning models, the tree-based models based on TextCNN + word2vec generally perform quite well, which proves the effectiveness of text feature extraction. Among the tree-based models, random forest obtains the best results, outperforming the other models in F1-score, precision, and recall.

Our model outperforms Benchmark 1 and Benchmark 2 using features in terms of almost all the indicators. The results of our model exceed random forest by 3% in precision and 6% in AUC, which illustrates the usefulness of adversarial networks in MSNs. In Benchmark 2, Zhang et al.'s method and Lyu et al.'s method both perform slightly worse than our method despite the use of location-based features. This further demonstrates that the interference of the difference of domain distribution affects the final results. Compared to the other models, our model does not use any additional features, and the generalization of our model is enhanced.

5.4. Ablation Study. In this part, we perform ablation experiments for our model. The ablation experiments compare two additional models: the non-text feature model (nTFM) and the non-adversarial model. The nTFM model contains user features and interaction information, while the non-adversarial model does not implement a GAN, but deploys a Sybil detector only using the TextCNN model combined with a neural network classifier.

The experimental results are shown in Figure 6. The overall performance of our proposed model is better than that of the non-adversarial model in terms of AUC, precision, recall, and F1-score. The AUC of our model with GANs is similar to the model of nTFM. However, all other metrics are improved significantly, which indicates that our model has better generalizability for detecting Sybil reviews. For all the metrics, the results of the non-adversarial model are lower than the results of the adversarial networks, but they perform slightly better than the model of nTFM in terms of generalization.

In order to show the difference between GANs and the non-adversarial model for text feature extraction, we use t-SNE [32] to reduce the dimensionality of the classification results and then perform visualization. The final results are shown in Figure 7. Compared to GANs, the classification results of the non-adversarial model are more compact and the distances between positive and negative samples are closer. This means that there is little difference between a normal Sybil review and a normal review in the non-adversarial model. In contrast, the discriminability of the text features learned by GANs is better, with a larger interval between samples with different labels. This is because the domain classifier tries to eliminate the dependency between the feature representation and the product category during the training phase. With the assistance of the minimax game, the Sybil detector can learn invariant features in different categories and obtain the capability of generalization.

5.5. Parameter Analysis. In this section, we discuss the impact of various parameters on our model. For the feature extractor of our model, we discuss the effect of window size z . For our final model based on GANs, we focus on the impact of the loss weight λ and the learning rate r in the loss function on the overall model.

5.5.1. The Impact of Window Size. The experimental results for different window sizes are shown in Table 2. When the window size is set from 1 to 5, we can best extract text features with different granularity. For other window sizes, either the results will be degraded due to missing features or the effective features will be degraded due to too large window size. For a specific window size, our model has n different filters. Considering the size of the training set, we set n to be 20 in order to reduce the training time while ensuring the training results.

5.5.2. The Impact of Loss Weight. In our GANs, λ is the critical parameter that regulates the importance of the two classification tasks. Larger λ indicates a higher importance of the product category classification task, while smaller λ indicates a higher importance of the Sybil review detection task. The value of λ determines the overall performance of the model, so we research the optimal value through a large number of experiments, which are shown in Table 3.

Based on our experiments on λ, we can study the impact of the auxiliary classification task of GANs on the overall

Table 1: The comparison results of different models.

Methods	Precision	Recall	F1-score	AUC
LR (TF-IDF)	0.49	0.59	0.53	0.55
XGBoost (word2vec + TextCNN)	0.63	0.64	0.63	0.66
AdaBoost (word2vec + TextCNN)	0.70	0.59	0.64	0.62
Random forest (word2vec + TextCNN)	0.76	0.77	0.77	0.76
SVM (TF-IDF)	0.74	0.71	0.73	**0.82**
KNN (TF-IDF)	0.73	0.75	0.74	0.66
TFM	0.66	0.68	0.67	0.79
Zhang et al.'s method [31]	0.70	0.68	0.69	0.79
Lyu et al.'s method [16]	0.72	0.74	0.73	0.80
Our model (word2vec + TextCNN + GANs)	**0.79**	**0.80**	**0.80**	**0.82**

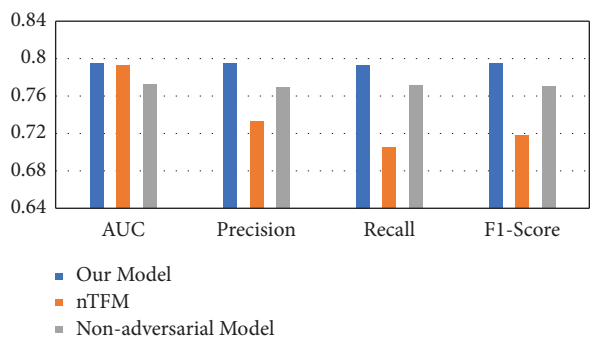

Figure 6: Results of ablation study on different models.

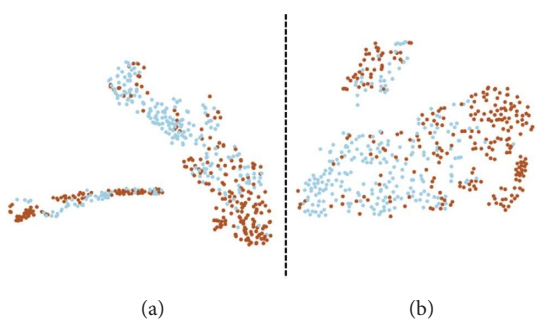

Figure 7: The final extracted features of the non-adversarial model (a) and GANs (b).

Table 2: Results on different window sizes.

Size of window	AUC	Precision	Recall	F1-score
1	0.652	0.63	0.643	0.636
2	0.7	0.72	0.723	0.721
3	0.725	0.721	0.725	0.723
4	0.722	0.723	0.721	0.722
1, 2	0.750	0.752	0.753	0.752
1, 2, 3	0.780	0.777	0.772	0.774
1, 2, 3, 4	0.782	0.78	0.779	0.779
1, 2, 3, 4, 5	0.785	0.782	0.783	0.782
1, 2, 3, 4, 5, 6	0.778	0.78	0.773	0.776
2, 3, 4, 5	0.775	0.768	0.78	0.774

model. When λ is set to zero, it means that the module of domain classifier fails, and its classification result has no effect on the feature extraction based on TextCNN. Hence, the overall model can be considered as a simple TextCNN for Sybil detection task. It can be found that even a simple TextCNN model can achieve good results for Sybil attack detection. As λ gradually increases, the experimental results of the model are gradually improving. If $\lambda = 0.95$, our model obtains the best classification performance, which proves that the introduction of the domain classification task helps improve the generalization ability of our model. When λ continues to increase, our model pays more attention to the accuracy of the classification task of review domains, resulting in insufficient information for the Sybil detection task. When the value of λ is particularly large, it is equivalent to the model completely turning into a domain classification model. In this case, the objective becomes to classify reviews into different categories, which leads to poor final results of the model.

Table 3: Results on different model weights.

λ	AUC	Precision	Recall	F1-score
0	0.773	0.771	0.772	0.771
0.1	0.776	0.775	0.776	0.775
0.5	0.778	0.776	0.78	0.778
0.8	0.78	0.78	0.779	0.779
0.9	0.788	0.788	0.781	0.784
0.95	0.795	0.796	0.800	0.798
1	0.782	0.780	0.781	0.780
1.05	0.780	0.780	0.780	0.780
1.1	0.778	0.78	0.773	0.776
1.5	0.772	0.771	0.771	0.771
2	0.76	0.758	0.76	0.759
10	0.71	0.703	0.701	0.702
100	0.62	0.617	0.62	0.618
10000	0.433	0.435	0.433	0.434

5.5.3. The Impact of Learning Rate. We also experimentally determine the optimal learning rate of the model. As an important parameter in supervised learning and deep learning, the learning rate determines whether and when the objective function converges to a local minimum. The convergence process will be slow when the learning rate is small, while the gradient may vibrate when the learning rate is large. A suitable learning rate can make the objective function converge to a local minimum in a suitable time.

Table 4: Results on different learning rates.

Learning rate	AUC	Precision	Recall	F1-score
1	0.522	0.513	0.520	0.516
0.1	0.676	0.677	0.678	0.677
0.01	0.748	0.750	0.749	0.749
0.001	0.780	0.780	0.776	0.778
5e − 4	0.788	0.788	0.781	0.784
1e − 5	0.788	0.789	0.780	0.784
Learning rate decay (from 1e − 3 to 1e − 5)	0.787	0.785	0.783	0.784
Adam	0.792	0.788	0.790	0.789
Adam + learning rate decay (from 1e − 3 to 1e − 5)	0.795	0.796	0.800	0.798

To compare the effects on the model results between different learning rates, the parameters other than the learning rate are consistent with the optimal results discussed above, and our experimental results are shown in Table 4. In addition to the fixed learning rate approach, we also discuss two optimization methods based on learning rate decay (learning rate decay and Adam + learning rate decay). The dynamic learning rate decay method decreases the learning rate as the epoch increases, which reduces the possibility of model oscillations and allows the gradient to converge to a stable range. Adam optimizer adaptively adjusts the learning rate and optimizes the results according to the gradient changes. In terms of learning rate decay, we set the initial learning rate to 1e-3 and make it decrease gradually with the number of iterations. The experimental results show that using learning decay alone cannot improve the model performance. By adding the Adam optimizer, all the performances of metrics improve, with F1-score improving by 1.5% compared to the optimal fixed learning rate model. Therefore, we suggest using Adam + learning decay as the optimizer.

6. Conclusion

In this paper, we propose a novel Sybil detection model based on GANs for MSNs, which contains a feature extractor, a domain classifier, and a Sybil detector. First, we construct the feature extractor with the neural network model of TextCNN, which is able to extract the text features of reviews. Second, we introduce the domain classifier to learn common features of reviews in different domains. Third, we design the Sybil detector to detect the Sybil review. Finally, we design our model based on GANs using the minimax game between the domain classifier and the Sybil detector. We also examine the effect of the two classification tasks of GANs and then find the optimal adversarial parameters for our model. Based on the dataset from Dianping, we experimentally validate that our model has excellent generalizability and achieves better detection accuracy than other Sybil detection models as well. In the future research, we will try to introduce graph neural networks to provide more properties for our model.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by JSPS KAKENHI (grant no. JP20K14742), Project of Cyber Security Establishment with Inter University Cooperation; National Natural Science Foundation of China (grant nos. 62102303, 61902351, and 61902353); Key R&D Program of Shaanxi Province (grant no. 2021KWZ-04); the Zhejiang Provincial Natural Science Foundation of China (grant nos. LY21F020022 and LY21F020023); Fundamental Research Funds for the Central Universities (no. 2022110161).

References

[1] D. Yuan, Y. Miao, N. Z. Gong et al., "Detecting fake accounts in online social networks at the time of registrations," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1423–1438, London UK, November 2019.

[2] J. Song, S. Lee, and J. Kim, "Crowdtarget: target-based detection of crowdturfing in online social networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 793–804, Denver Colorado USA, October 2015.

[3] A. Ramachandran, N. Feamster, and S. Vempala, "Filtering spam with behavioral blacklisting," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 342–351, Alexandria Virginia USA, October 2007.

[4] W. Wei, F. Xu, C. C. Tan, and Q. Li, "Sybildefender: defend against sybil attacks in large social networks," in *Proceedings of the 2012 IEEE INFOCOM*, pp. 1951–1959, IEEE, Orlando FL USA, March 2012.

[5] S. Effendy and R. H. Yap, "The strong link graph for enhancing sybil defenses," in *Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 944–954, IEEE, Atlanta GA USA, June 2017.

[6] S. Furutani, T. Shibahara, K. Hato, M. Akiyama, and M. Aida, "Sybil detection as graph filtering," in *Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, Taipei Taiwan, December 2020.

[7] J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai, "Votetrust: leveraging friend invitation graph to defend against social network sybils," in *Proceedings of the 2013 Proceedings IEEE INFOCOM*, pp. 2400–2408, IEEE, Turin, Italy, April 2013.

[8] H. Zhang, J. Zhang, C. Fung, and C. Xu, "Improving sybil detection via graph pruning and regularization techniques," in *Proceedings of the Asian Conference on Machine Learning. PMLR*, pp. 189–204, Hong Kong, November 2016.

[9] M. Bao, J. Li, J. Zhang, H. Peng, and X. Liu, "Learning semantic coherence for machine generated spam text detection," in *Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, Budapest, Hungary, July 2019.

[10] H. Ahmed, I. Traore, and S. Saad, "Detecting opinion spams and fake news using text classification," *Security and Privacy*, vol. 1, no. 1, p. 9, 2018.

[11] F. Zhang, L. Qiu, P. Qi, and H. Luo, "A novel text features jointing model for review spam filtering of Chinese," in *Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 2051–2056, IEEE, Limassol, Cyprus, June 2020.

[12] J. Ding, Z. Liu, S. Xiao et al., "Beyond the click: a first look at the role of a microblogging platform in the web ecosystem," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 743–754, 2019.

[13] M. Rahman, B. Carbunar, J. Ballesteros, G. Burri, and D. H. Chau, "Turning the tide: curbing deceptive yelp behaviors," in *Proceedings of the 2014 SIAM International Conference on Data Mining SIAM*, pp. 244–252, Philadelphia, PA, USA, April 2014.

[14] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, *Compa: Detecting Compromised Accounts on Social Networks*Carnegie Mellon University, Pittsburgh, PA, USA, 2013.

[15] X. Zhang, H. Xie, and J. C. Lui, "Sybil detection in social-activity networks: modeling, algorithms and evaluations," in *Proceedings of the 2018 IEEE 26th International Conference on Network Protocols (ICNP)*, pp. 44–54, IEEE, Cambridge, UK, September 2018.

[16] C. Lyu, D. Huang, Q. Jia et al., "Predictable model for detecting sybil attacks in mobile social networks," in *Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, Nanjing, China, March 2021.

[17] I. Goodfellow, J. Pouget-Abadie, M. Mirza et al., "Generative adversarial nets," *Advances in Neural Information Processing Systems*, vol. 27, 2014.

[18] A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, "Adversarial autoencoders," 2015, https://arxiv.org/abs/1511.05644.

[19] Z. C. Lipton and S. Tripathi, "Precise recovery of latent vectors from generative adversarial networks," 2017, https://arxiv.org/abs/1702.04782.

[20] Y. Ganin and V. Lempitsky, "Unsupervised domain adaptation by backpropagation," in *Proceedings of the International Conference on Machine Learning. PMLR*, pp. 1180–1189, Lille, France, July 2015.

[21] Y. Pu, S. Dai, Z. Gan et al., "Jointgan: multi-domain joint distribution learning with generative adversarial nets," in *Proceedings of the International Conference on Machine Learning. PMLR*, pp. 4151–4160, Stockholmsmässan, Stockholm Sweden, July 2018.

[22] Z. Qu, C. Lyu, and C.-H. Chi, "Mush: Multi-Stimuli Hawkes Process Based Sybil Attacker Detector for User-Review Social Networks," *IEEE Transactions on Network and Service Management*, 2022.

[23] J. Gu, G. Wang, J. Cai, and T. Chen, "An empirical study of language cnn for image captioning," in *Proceedings of the IEEE International Conference on Computer Vision*, pp. 1222–1231, Cambridge, MA, USA, June 1995.

[24] K. Chandrasegaran, N.-T. Tran, and N.-M. Cheung, "A closer look at fourier spectrum discrepancies for cnn-generated images detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 7200–7209, Seattle, WA, USA, June 2021.

[25] Y. Zhang and B. Wallace, "A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification," 2015, https://arxiv.org/abs/1510.03820.

[26] B. Guo, C. Zhang, J. Liu, and X. Ma, "Improving text classification with weighted word embeddings via a multi-channel textcnn model," *Neurocomputing*, vol. 363, pp. 366–374, 2019.

[27] C. Zhang, R. Guo, X. Ma, X. Kuai, B. He, and W-textcnn, "W-TextCNN: a TextCNN model with weighted word embeddings for Chinese address pattern classification," *Computers, Environment and Urban Systems*, vol. 95, Article ID 101819, 2022.

[28] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[29] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 2687–2700, 2021.

[30] H. Han, L. Fang, W. Lu, W. Zhai, Y. Li, and J. Zhao, "A gcica grant-free random access scheme for m2m communications in crowded massive mimo systems," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6032–6046, 2022.

[31] X. Zhang, H. Zheng, X. Li, S. Du, and H. Zhu, "You are where you have been: sybil detection via geo-location analysis in osns," in *Proceedings of the 2014 IEEE Global Communications Conference*, pp. 698–703, IEEE, Austin, TX, USA, December 2014.

[32] L. Van der Maaten and G. Hinton, "Visualizing non-metric similarities in multiple maps," *Machine Learning*, vol. 87, no. 1, pp. 33–55, 2012.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8954767, 13 pages
https://doi.org/10.1155/2022/8954767

Research Article

New Constructions of Existential Unforgeable Aggregate Signature Scheme from CSP

Bo Mi,[1] **Yongxing Zou**,[1] **Darong Huang**,[1] **Yang Liu**,[1] **and Lu Chen**[2]

[1]*School of Information Science and Engineering, Chongqing Jiaotong University, Chongqing, China*
[2]*Naval University of Engineering, Wuhan, China*

Correspondence should be addressed to Yongxing Zou; yongxing_zou1998@163.com

Received 29 July 2022; Revised 8 September 2022; Accepted 22 September 2022; Published 9 November 2022

Academic Editor: Lei Liu

In future, hundreds of years of mathematical problems that the security of public key cryptography algorithms rely on may be defeated by quantum algorithms. How can a digital signature scheme gracefully balance security and efficiency? This study uses the conjugate search problem and the left self-distributive system to combine and uses the RSA-like algorithm as the underlying structure to propose a new aggregated signature scheme. We, through the EUF game, under the random metaphor model, prove that the security of the scheme satisfies the adaptation unforgeability under selective message attack, the scheme can be finally reduced to the discrete logarithm problem or large prime number decomposition problem. In addition, we can achieve anti-quantum attack and exhaustive attack by performing matrix calculations on the message, defining and changing the structure of the matrix by encoding, and setting thresholds for the matrix dimension and the length of the private key. In terms of efficiency, the message signature implementation is linear compared with the expansion rate in terms of storage and computing overhead, and the generation and verification of the final signature pair have nothing to do with the number of users. In addition, the length of the signature is fixed and the size is only the length of a single group, which effectively reduces the generation of public and private key pairs and saves a lot of storage space. The storage space and computational complexity are also effectively improved compared with other solutions.

1. Introduction

Throughout the ages, information security has played an important role in both ordinary life and military strategy. Cryptography provides the theory and technical support of information security and meets the four requirements of information security from the two aspects of data encryption and digital signature: confidentiality means information content cannot be accessed by unauthorized persons. Integrity means no information modification during transmission and storage. Authentication means identification and authentication service technology applied to both the entity and the information itself. Nonrepudiation means users cannot deny their existing actions and commitments [1–3]. Among them, data encryption can realize the confidentiality of data, and a digital signature can realize the integrity, authentication, and nonrepudiation of information. The digital signature is a digital simulation of a handwritten signature. With the advent of the information age, most standard protocols, and software support digital signatures, at present, many countries have legislation that stipulates that digital signatures and handwritten signatures have the same legal effect. In 1978, Rivest et al. realized the first public-key encryption scheme [4] for the large integer factorization problem, and at the same time, using this public-key encryption scheme, we realized the first digital signature scheme, namely, the famous RSA scheme. Since the proposal of this scheme, the research on digital signatures has always been one of the main research topics and hotspots in the field of cryptography. Digital signatures often involve multiuser scenarios: on the one hand, the signature itself needs to be signed by multiple users; on the other hand, although the signature is generated by a single user, security in a multiuser environment needs to be considered. Boneh

et al. first proposed the concept of aggregated signatures in 2003 [5] and constructed the first aggregated signature scheme using pairings on elliptic curves. Roughly speaking, the aggregated signature σ is the synthesis of n different signatures by n users to different pairs of documents $m_1, m_2, \ldots, m_n$ into a single signature σ, which reduces not only the storage space requirements for signatures but also the requirements for transmission network bandwidth. At the same time, the verification of multiple signatures is simplified into one verification, which reduces the workload of the verifier. Especially, in some computing resources and a large number of fast authentication situations at the same time, such as online ticket purchases, virtual currency, safety routing protocol, and vehicle ad hoc networks, whether it is the Spring Festival transport of 1.4 billion people in China or the routing topology in a certain area, it has a greater application demand for short-signed fast algorithms. In the direction of protecting user data privacy and communication security, even 6 G networks with endogenous security face many problems, such as AI-induced concerns about security and privacy issues, including data security, AI model and algorithm security, and malicious use of AI technology. Traditional computational complexity-based cryptographic mechanisms (such as encryption, authentication, authorization, signature, and privacy protection) will remain the primary method for maintaining network security and data privacy. However, due to the characteristics of 6 G networks, lightweight and efficient encryption and signature mechanisms are very popular. The combination of 6 G and blockchain, through the application of encryption algorithms such as aggregate signature and ring signature in the data structure, makes the data highly anonymous and improves the efficiency of authentication, which is also a promising solution. The achievement of these goals requires an efficient and secure signature algorithm as the underlying technical support. In the near future, quantum computers are expected to break the modern public key cryptosystem. Postquantum cryptography must be an important means to protect future information security. The past cryptosystems cannot be abandoned. How to migrate from public key cryptosystems to postquantum cryptosystems has become a hot topic.

1.1. Contributions. Given the problems of existing schemes such as excessive storage signature overhead, low signature verification efficiency, insufficient security, and inability to achieve antiquantum computing in the future, we propose a new scheme; the main contributions of this study are summarized as follows:

(1) This study uses the combination of RSA, CSP (conjugate search problem), and LD (left self-distributive system) to construct a new aggregated signature scheme, and we utilize the RSA-like as the underlying structure of the scheme, which can eventually be reduced to the DLP problem or the large prime number decomposition problem because the RSA algorithm is based on the large prime number decomposition problem.

(2) In terms of security, the proposed scheme satisfies that EUF-CMA can resist existential forgery attacks under adaptive selection messages. Through the EUF game, adversary A uses his scheme to attack the challenger as a subroutine, designs computational targets for adversary B, and then defines the advantage that B can solve for a given RSA-like scheme to achieve the proof.

(3) In terms of efficiency, since all messages are encoded as low-dimensional matrices with a certain regularity, and with the help of the characteristics of the CSP-LD system, the signatures of all signers will be synthesized into the final unique signature through calculation.As a result, the signature storage and verification become more efficient. The overhead is greatly reduced, the expansion rate of message signature implementation is linear compared with the storage and computing overhead, and the length of the final aggregated signature is fixed, which saves the maximum amount of signed storage space without losing accuracy.

(4) What is more prominent is that the scheme we propose can customize the format of the encoded message matrix. By setting the system parameters to reach a certain threshold, it can achieve antiquantum attacks. Other problems using RSA or DLP include digital signature schemes based on pairing problems, neither can resist the quantum computer attack under Shor's algorithm.

2. Related Work

How to construct efficient and secure aggregated signatures has always been highly concerning for cryptographers. Hashimoto and Ogata [6] proposed the first unrestricted and compact aggregated signature scheme, in which the signature size is constant, and the generated pair signatures can have different information states and can aggregate any combination of signatures. Iwasaki et al. [7] extended from the two perspectives of structured signature and identity-based signature and constructed an identity-based structured aggregated signature scheme, and the security of the scheme will not be reduced due to the ability of the adversary. It can successfully defend against switching attacks (CCS 2007, Boldyreva et al. [8]) and reordering attacks (ISPEC 2007, Shao [9]). In recent years, the combination of signature scheme and blockchain technology [10–12], federated learning technology [13], 6G network [14], homomorphic learning [15], network routing protocol [16], edge computing [17], vehicular ad hoc networks [18], and software-defined vehicular network [19–21] by applying signature algorithms and encryption algorithms to the experimental scheme to further strengthen the security of the scheme and improve the privacy protection capability of the scheme is also a hot topic. In the blockchain, the digital signature is one of the three basic technologies, and its importance is self-evident. The blockchain mainly uses digital signatures to control permissions, identify the legal

identity of transaction initiators, and prevent malicious nodes from impersonating. Coincidentally, the distributed and decentralized edge nodes inherent in the 6 G network allow blockchain technology to be used to improve the endogenous security performance of 6 G, based on blockchain technology to achieve what is considered a promising solution in the field of data security and privacy in 6 G networks. Data have a high level of anonymity by applying encryption algorithms such as aggregate signature signatures and ring signatures in the data structure. In edge computing, federated learning, and homomorphic learning, edge computing processes and applies data to the nearest computing facility to protect its privacy or federated learning uses other remote data and protects the privacy of remote data, and at the same time collaborative modeling, or the cloud computing model based on homomorphic encryption, solves the problem of users trusting cloud service providers not to steal or even user data and to achieve data confidentiality and computability. Verifying the identity legitimacy of a user or terminal based on a digital signature is both basic and necessary work. SDVN (software-defined virtual network) is a new type of VANET (vehicle ad hoc network), a promising networking paradigm, that can provide intelligent information exchange by separating network management and data transfer. For such applications that combine vehicles with networks, frequently changing topology networks, real-time routing calculations, and efficient service requests all play a crucial role in vehicle networks. Before designing a routing strategy for vehicles in these operations, it is undoubtedly a wise move to use an aggregated signature scheme that is fast and can protect its identity privacy to verify the legitimacy of vehicle units. Domestic Li et al. [22] constructed an efficient aggregated signature scheme under the certificateless public-key cryptosystem based on bilinear pairing, and the signature length of the scheme is only two group elements. Only 4 pair operations (of constant magnitude) and n scalar multiplication operations are required in signature verification, which has a fast signature verification algorithm and fast transmission efficiency. Zhou et al. [23] proposed two certificateless aggregated signature schemes that do not use bilinear mapping for different network environments. However, due to the long aggregate signature length of Scheme I, it can only be used in a network environment with high bandwidth and the final signature length is positively correlated with the number of users, Scheme II has a shorter signature length, and the length has nothing to do with the number of users and will be used in a network environment with low bandwidth. Whether the security proofs of these two schemes have existential unforgeability under adaptive chosen message attack remains to be further analyzed. At present, most aggregated signature schemes are constructed according to the pairings on elliptic curves. For example, Yang et al. [24], aiming at the problems of privacy leakage and low signature verification efficiency in VANET (vehicular ad hoc network), combined with identity-based cryptography and aggregated signature technology, designed a message authentication scheme for VANET to improve the security of the system and the efficiency of road traffic.

However, there are still many deficiencies in the pairing-based scheme: one is that the hardware devices currently implemented are all oriented towards RSA and DLP (discrete logarithm problem), and the pairing-based cryptography scheme still has a long way to go before it can be applied in reality. Another is that the pairing problem was not introduced into cryptography for research until 2000. Unlike RSA and DLP problems, hundreds of years of research have made them well-understood in the cryptography community. Therefore, most of the current digital signature schemes are based on the discrete logarithm problem and the RSA problem. For example, many people learn from the ideas of Bellare and Neven [25] and propose RSA-based identity-based sequential signature schemes, which need to be further strengthened and improved in terms of the storage efficiency of signatures and whether they can achieve EUF-CMA (existential unforgeability under adaptive chosen message attack) security. What makes us more motivated is that almost no one aggregates signatures based on RSA.

More importantly, with the development of quantum computers, the abovementioned mathematical problems that the security of public key cryptographic algorithms depends on can be solved by efficient quantum algorithms [26, 27]. As the underlying mathematical problems are solved, including discrete logarithms (elliptic curve versions) and large integer factorization, all these public key cryptographic algorithms will no longer be secure, which directly affects Diffie-Hellman, Elliptic Curve, RSA, and those currently used algorithms. In 2016–2017, NIST focused on the solicitation of the following three categories of postquantum cryptographic algorithms: encryption, key exchange, and digital signatures. Among the 69 "complete and suitable" candidate drafts, postquantum cryptographic algorithms constructed by the following 4 mathematical methods are mainly included lattice-based, code-based, multivariate-based, and hash-based. The scheme discussed in this study does not have a self-made wheel, but through the fusion of CSP and matrix, using the encoding of the message to achieve antiquantum attacks, the specific form is in the follow-up content.

3. Preliminaries

Before introducing definitions, let us review the concept of groups.

When an algebraic system has a certain operation $\langle G, * \rangle$, $*$ is a binary operation. When $*$ satisfies the following properties, we call the algebraic system a group, in which $\langle G, * \rangle$ is simply denoted as G:

(1) Closedness: it means for $\forall a, b \in G$ satisfying $a * b \in G$.

(2) Unitary: it means, for $\forall a \in G, \exists e$, there are existing $a * e = e * a = a$. At the same time, we call e the identity element of $\langle G, * \rangle$.

(3) Inverse element exists: it means, for $\forall a \in G, \exists b \in G$, there are existing $a * b = b * a = \mathrm{e}$. Then, b is called the inverse of a, denoted as a^{-1}.

(4) Associativity: it means $\forall a, b, c \in G$ satisfying $(a * b) * c = a * (b * c)$.

An algebraic system $\langle G, * \rangle$ is called a semigroup if it only satisfies closure and associativity. For example, multiplication and addition of real numbers. If the $*$ operation in an algebraic system $\langle G, * \rangle$ also satisfies the commutative law, that is, $\forall a, b \in G$ has $a * b = b * a$, then $\langle G, * \rangle$ is called a commutative group, also called an Able group.

Note that not all elements in G have inverses. At the same time, $a^n = a * * * a$, n times, and $a^{-n} = b * * * b$, n times, where $n > 1$.

Let G^{-1} be the set of all invertible elements belonging to G, expressed as follows:

$$G^{-1} = \{a \in G\colon \exists b \in G, \text{ so that } a * b = b * a = e\}. \tag{1}$$

The so-called CSP problem can be roughly explained in the group: there is a group G, where $a \in G$ and $x \in G^{-1}$; there must be an element $b \in G$; a and b are isomorphic so that $b = xax^{-1}$; we say that, for the element x, a, and b are conjugated.

Definition 1 (conjugacy search problem, CSP). Suppose G is a noncommutative group, a and b are two elements belonging to G, denoted as $a, b \in G$, and the unknown x is an element in G^{-1}, denoted as $x \in G^{-1}$, satisfying $b = xax^{-1}$. The so-called CSP (conjugate search problem) problem in the noncommutative group G refers to finding another x' in G^{-1}, denoted as $x' \in G^{-1}$, so that $b = x'ax'^{-1}$, where x' does not need to be exactly the same as x.

Lemma 1. *The same applies to transforming a and b into matrix form in the above search problem. For example, write a and b as the simplest two-dimensional upper triangular matrix:*

$$a = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}, b = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}. \tag{2}$$

Satisfying $b = xax^{-1}$,

$$b = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \begin{pmatrix} \frac{1}{x_1} & -\frac{x_2}{x_1 x_3} \\ 0 & \frac{1}{x_3} \end{pmatrix}. \tag{3}$$

CSP (conjugate search problem) problem in the noncommutative group G refers to finding another x' in G^{-1}, denoted as $x' \in G^{-1}$, so that $b = x'ax'^{-1}$, where x' does not need to be exactly the same as x:

$$x' = \begin{pmatrix} x_1' & x_2' \\ 0 & x_3' \end{pmatrix}. \tag{4}$$

Theorem 1. *If the matrix A is invertible, then the inverse matrix of A is unique, and the proof is omitted.*

Definition 2 (left self-distributive system, LD [28]). W is a nonempty subset and F is a complete and closed function satisfying $F\colon W \times W \longrightarrow W$; we denote $F(a, b)$ as $F_a(b)$. If F satisfies the following formula, then we call $F(\cdot)$ a left self-distributive system or LD system for short:

$$F_r(F_s(p)) = F_{F_r(s)}(F_r(p)), \quad (\forall p, r, s \in W). \tag{5}$$

If we consider $F_r(s)$ as a binary operation $r * s$, the above expression becomes

$$r * (s * p) = (r * s) * (r * p). \tag{6}$$

The operator $*$ is left self-distributive.

Definition 3 (CSP-LD system [29]). Assuming that G is a noncommutative group, the binary function F satisfies the following conjugation operations:

$$F\colon G^{-1} \times G \longrightarrow G, \quad (a, b) \longrightarrow aba^{-1}. \tag{7}$$

Then, $F(\cdot)$ is a CSP-LD system.

The proof is as follows:

$$\begin{aligned} F_r(F_s(p)) &= F_r\left(sps^{-1}\right) = rsps^{-1}r^{-1} \\ &= rsr^{-1} \cdot rpr^{-1} \cdot rs^{-1}r^{-1} \\ &= rsr^{-1} \cdot rpr^{-1} \cdot \left(rsr^{-1}\right)^{-1} \\ &= F\left(rsr^{-1}, rpr^{-1}\right) = F_{F_r(s)}(F_r(p)). \end{aligned} \tag{8}$$

The CSP-LD system also has some very simple but very useful properties in the field of cryptography. A few are listed below, and readers can prove it by themselves.

Property 1: $F_a(a) = a, a \in G^{-1}$

Property 2: $F_a(b) = c \Leftrightarrow F_{a^{-1}}(c) = b, a \in G^{-1}, b \in G$

Property 3: $F_a(bc) = F_a(b)F_a(c), a \in G^{-1}, b, c \in G$

The power-law property of F in the CSP-LD system will be described in detail below.

Lemma 2. *Suppose a and b are given and fixed, $a \in G^{-1}$ and $b \in G$. Then, for any three integers m, s, t, as long as $m = s + t$ is satisfied, there must be the following formula:*

$$\begin{aligned} &F_a(b^m) = F_a(b^s)F_a\left(b^t\right) = F_a^m(b) \\ &F_{a^m}(b) = F_{a^s}(F_{a^t}(b)) \end{aligned}. \tag{9}$$

The first proof of the formula is as follows:

$$\begin{aligned} F_a(b^m) &= ab^m a^{-1} = ab \cdots\cdots ba^{-1} \\ &= aba^{-1} \cdot aba^{-1} \cdots\cdots aba^{-1} \\ &= \left(aba^{-1}\right)^m = F_a^m(b). \end{aligned} \tag{10}$$

The second proof of the formula is as follows:

$$\begin{aligned} F_{a^m}(b) &= a^m b a^{-m} = a^s a^t b a^{-t} a^{-s} \\ &= a^s F_{a^t}(b) a^{-s} = F_{a^s}\left(F_{a^t}(b)\right). \end{aligned} \tag{11}$$

The two formulas are of great help to our follow-up content. One satisfies the internal and external exchange of power, transforming the exponent of the variable into the exponent of the function, and the other satisfies the addition of the power law.

Definition 4 (security definition of EUF-CMA). Currently, there are two main types of attacks against digital signatures: key-only attacks and known-message attacks. A key-only attack means that the adversary only knows the signer's public key without any other message. Among the many known-message attacks, the attack method with the highest attack strength is called adaptively chosen message attacks. In this type of attack, the adversary uses the signer as a querier, which can query not only the challenger for messages that depend on the signer's public key but also the signed message that has already been queried. If a signature scheme still has signature unforgeability under this attack, in other words, the signature constructed by the adversary through this optional challenge is still illegal and cannot be verified, the scheme is said to have existential unforgeability under adaptive chosen message attack, which is referred to as EUF-CMA security [30, 31]. The advantage of the adversary A in the following experiments is negligible:

$$\begin{aligned} &\mathrm{Exp}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k): \\ &(vk, sk) \leftarrow \mathrm{SigGen}(k), \\ &(M, \sigma) \leftarrow A^{\mathrm{Sign}_{sk}(\cdot)}(vk). \end{aligned} \tag{12}$$

Let Q denote that A accesses the message set of signature metaphor $\mathrm{Sign}_{sk}(\cdot)$.

Returns 1 if $\mathrm{Vrfy}_{vk}(M, \sigma) = 1\hat{M} \in \neq Q$, otherwise returns 0, where A has access to the signed idiom machine polynomial bounded q_H degree. The specific meaning is whether the challenger can judge whether the signature σ of the message M comes from the message set of the signature metaphor $\mathrm{Sign}_{sk}(\cdot)$ visited by the adversary A through $\mathrm{Vrfy}_{vk}(M, \sigma)$. If it returns 1, it means that the challenger believes that the signature σ of the message M is naturally generated by legal means. If it returns 0, it means that the challenger believes that the signature σ of the message M is generated by A accessing the metaphor $\mathrm{Sign}_{sk}(\cdot)$.

The advantage of A is defined as follows:

$$\mathrm{Adv}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = \left|\Pr\left[\mathrm{EXP}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = 1\right]\right|. \tag{13}$$

When $\mathrm{Adv}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) < \mathrm{negl}(k)$, which is a negligible function, then we say the scheme is EUF-CMA safe.

4. EUF-CMA Security Signature Scheme Based on CSP

We first review the basic process of the RSA algorithm and specifically prove why the classical RSA signature algorithm does not have the existence of unforgeability under the adaptive chosen message attack.

The basic description of the RSA-like signature algorithm is as follows.

(1) Key generation is as follows:

$$\begin{aligned} &\mathrm{GenRSA}(k): \\ &p, q \leftarrow \mathrm{GenPrime}(k), \\ &N = pq, \varphi(n) = (p-1)(q-1), \\ &\text{Choose } e, \text{ for } 1 < e < \varphi(n) \text{and } (\varphi(n), e) = 1, \\ &\text{Calculate } d, \text{ for } d \cdot e \equiv 1 \bmod \varphi(n), \\ &pk = (n, e), sk = (n, d). \end{aligned} \tag{14}$$

(2) Signature is as follows:

$$\begin{aligned} &\mathrm{Sign}_{sk}(M): \\ &\sigma = M^d \bmod n. \end{aligned} \tag{15}$$

(3) Verify is as follows:

$$\begin{aligned} &\mathrm{Vrfy}_{pk}(M, \sigma): \\ &\text{Return } 1, \text{if } \sigma^e = M \bmod n, \text{otherwise return } 0. \end{aligned} \tag{16}$$

Obviously, this signature algorithm is not antiforgery under the adaptive chosen message attack. When the attacker A performs a q_H-bounded query, A can submit $M_i = r^e \cdot M$ for the signature query. At this point, the challenger answers, computes $u_i = M_i^d \bmod n, i = 1, 2, \ldots, q$, and returns it to A. A forges the signature of message M and outputs $(M, \sigma) = (M, u_i/r)$ because of

$$u_i \equiv \left(r^e M\right)^d \bmod n \equiv r M^d \bmod n. \tag{17}$$

Therefore, $\sigma = u_i/r \equiv M^d \bmod n$ is the legal signature of M.

According to the previous Definition 4, EUF-CMA security definition, we can make the following analysis:

$$\begin{aligned} &\mathrm{Exp}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k): \\ &(vk, sk) \leftarrow \mathrm{SigGen}(k), \\ &(M, \sigma) \leftarrow A^{\mathrm{Sign}_{sk}(\cdot)}(vk). \end{aligned} \tag{18}$$

Let Q denote the message set of A accessing signature metaphor $\mathrm{Sign}_{sk}(\cdot)$, denoted as $M \in Q$, where A has access to the signed metaphor polynomial bounded q_H times.

At this time, the adversary A has the message M and its corresponding signature σ after accessing the signature machine $\mathrm{Sign}_{sk}(\cdot)$. At the same time, A calculates $M' = r^e \cdot M$, and the challenger calculates $u' = M'^d \bmod n$ and returns it to A. Then, A has another pair of signatures $(M, \sigma') = (M, u'/r)$. Verified by the challenger for legitimacy,

$$\sigma' = \frac{u'}{r} \equiv \frac{(r^e M)^d}{r} \bmod n \equiv \frac{rM^d}{r} \bmod n \equiv M^d \bmod n = \sigma. \quad (19)$$

However, the adversary A has not used M' to access the signature metaphor, so $M' \notin Q$. That is to say, the challenger believes that the message M signature σ' is naturally generated through legal means. The advantage of A at this time is defined as follows:

$$\mathrm{Adv}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = \left|\Pr\left[\mathrm{EXP}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = 1\right]\right| = 1. \quad (20)$$

How to solve this problem? The previous method is to use the FDH (global hash function) that the output bit length of the hash function is the same as the modulus bit length to ensure the security of the scheme [32], but the hash function itself is a relatively complex algorithm, and the so-called randomness itself is controversial. Because no algorithm is truly random, such as $h = H(m)$, whose output is a pseudorandom process from m to h. In addition, using a hash function will reduce the efficiency of the scheme. Below, we will propose a new solution that satisfies EUF-CMA and prove that its security is improved based on the comparison above.

4.1. Definition of the RSA Problem (RSAP). Given a positive integer n (n is the product of two different odd prime numbers p, q), a positive integer $e(\gcd(e, (p-1)(q-1)) = 1)$, and an integer c, we find an integer m such that $m^e \equiv c \bmod n$. That is to say, the RSA problem is to find the root of e times in the case of modulo n (n is a composite integer).

4.2. The Difficult Problem of CSP Based on DDH. G is a noncommutative group. Suppose F is a function that satisfies the above CSP-LD system while having an adversary A. For any $a \in G^{-1}$, $b \in G$, we perform the following two experiments in parallel:

$$\begin{array}{ll} \text{Experiment } \mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-real}} & \text{Experiment } \mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-rand}} \\ i \xleftarrow{\$} T, X \leftarrow F_{a^i}(b), & i \xleftarrow{\$} T; X \leftarrow F_{a^i}(b), \\ j \xleftarrow{\$} T, Y \leftarrow F_{a^j}(b), & j \xleftarrow{\$} T; Y \leftarrow F_{a^j}(b), \\ Z \leftarrow F_{a^{i+j}}(b), & L \xleftarrow{\$} T, Z \leftarrow F_{a^L}(b), \\ b \leftarrow A(X, Y, Z), & b \leftarrow A(X, Y, Z), \\ \text{Return } b. & \text{Return } b. \end{array} \quad (21)$$

For adversary A, the advantage of successful attacks in a CSP system based on the DDH assumption is defined as follows:

$$\mathrm{Adv}_{F,A}^{\mathrm{csp-ddh}} = \left|\Pr\left[\mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-real}} = 1\right] - \Pr\left[\mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-rand}} = 1\right]\right|. \quad (22)$$

In other words, when i, j, L are taken randomly from T, we can consider that $(F_{a^i}(b), F_{a^j}(b), F_{a^{i+j}}(b))$ and $(F_{a^i}(b), F_{a^j}(b), F_{a^L}(b))$ are computationally indistinguishable when distributed. At present, there is no specific statement in the academic community to judge whether the CSP-DDH problem is hard, but we know that, in a general cyclic group, the DLP problem and the DDH problem are equivalent. From the above CSP-LD system reasoning, we know that, on a noncommutative semigroup, the CSP problem and the CSP-DDH problem can be directly replaced by the DLP problem and the DDH problem. Therefore, by logical reasoning, we can conclude that in a general noncommutative semigroup, the CSP problem and the CSP-DDH problem are equivalents [27].

4.3. Digital Signature Scheme Based on CSP-LD System. Assuming that a and b are random numbers, $a \in G^{-1}$ and $b \in G$, which have been fixed for the system parameters. Assuming that G is a general noncommutative semigroup, the binary function F satisfies the following conjugate operations:

$$F\colon G^{-1} \times G \longrightarrow G, (a, b) \longrightarrow aba^{-1}. \quad (23)$$

We mark $F(a, b) = aba^{-1}$ as $F_a(b)$.

(1) Key generation is as follows:

$$\begin{aligned} p, q &\leftarrow \mathrm{GenPrime}(k), \\ N = pq, \varphi(n) &= (p-1)(q-1), \\ \text{Choose } e, \text{for } 1 < e < \varphi(n) &\text{and } (\varphi(n), e) = 1, \\ \text{Calculate } d, \text{ for } d \cdot e &\equiv 1 \bmod \varphi(n), \\ pk = (n, e), sk &= (n, d). \end{aligned} \quad (24)$$

(2) Signature is as follows:

$$\begin{aligned} &\mathrm{Sign}_{sk}(M): \\ &H = F_a(M), \\ &\sigma = H^d \bmod n. \end{aligned} \quad (25)$$

(3) Verify is as follows:

$$\begin{aligned} &\mathrm{Vrfy}_{pk}(M, \sigma): \\ &\text{Return } 1, if\ \sigma^e = H \bmod n, \text{ otherwise return } 0. \end{aligned} \quad (26)$$

Under the CSP-LD system, the above scheme RSA-CSP-LD is EUF-CMA safe if the GenRSA-related RSA problem is difficult. Compared with the predecessors using the global hash function FDH to map M to prevent signature forgery, our scheme has a more compact security reduction.

Theorem 2. *Specifically, assuming that there is an adversary A that breaks the RSA-CSP-LD scheme with the advantage of ε, then there must be an adversary B that solves the RSA problem at least with the advantage of the following:*

$$\mathrm{Adv}_B^{\mathrm{RSA}}(k) \geq \frac{\varepsilon(k)}{eq_s}. \quad (27)$$

Proof. The EUF game is as follows.

In this proof process, all references to G refer to a universal noncommutative group, F is the CSP-LD system function defined on G, and $a \in G^{-1}$ and $b \in G$ are two fixed elements.

(1) The challenger runs Key generation (k) to get (n, e, d) and runs CSP-LD to get $F_a(b)$. Adversary A gets the public key (n, e).

(2) The adversary A can ask the challenger $F_a^{(\cdot)}(b)$ and the signature of the message; when A requests the signature of the message M, the challenger returns $\sigma = F_a(b^{|M|})^d \bmod n$ to A.

(3) A outputs a message-signature pair (M, σ) where A has not previously requested a signature for a message M. If $\sigma^e = F_a(b^M) \bmod n$, the adversary attack is successful.

The following proves that the RSA-CSP-LD scheme can be reduced to the RSA problem.

The adversary B knows (n, e, y^*) where y^* is uniformly random on Z_n^*. Using A to attack RSA-CSP-LD as a subroutine, the goal is to calculate $(y^*)^{1/e} \bmod n$. Because if B can get σ such that $\sigma^e \equiv y^* \bmod n$, then $\sigma \equiv (y^*)^{1/e} \bmod n$. Because of $\sigma^e \equiv y^* \bmod n$, if y^* is the value of $F_a(M)$ of a message M in the CSP-LD system, then σ is the signature of the message. (M, σ) is generated by adversary A, but $F_a(M)$ is generated by B, and B can be set to $F_a(M) = y^*$. Since B does not know which message A generates a forged pair signature when generating y^*, B has to make a guess, where the jth query of A corresponds to the final forged result of A. Before the reduction, for the sake of generality, we assume that the adversary A will not issue the same query to $F_a(M)$ twice. If A requests the signature of M, we take that it has been asked $F_a(M)$ before.

The reduction process is as follows:

(1) B gives the public key (n, e) to A.

(2) $F_a(\cdot)$ inquiry (at most q_s times): B creates a list query, which is initially empty and the element type is a quadruple $(M_i, \sigma_i, y_i, c_i)$, indicating that B has set $F_a(M) = y_i$, $\sigma_i^e \equiv y_i \bmod n$. When A initiates a query (set to M), B will answer as follows:

(a) If there is already an item $(M_i, \sigma_i, y_i, c_i)$ corresponding to M in query, we reply with y_i.

(b) Otherwise, B randomly chooses a $c_i \leftarrow \{0, 1\}^R$ and sets $\Pr[c_i = 0] = \delta$.

If $c_i = 0$, we return y^*.

Otherwise, we select a random value $\sigma_i \leftarrow Z_n^{*R}$, calculate $y_i \equiv \sigma_i^e \bmod n$, take y_i as the answer to this query, and store $(M_i, \sigma_i, y_i, c_i)$ in the table query.

(3) Signature query (up to q_s times): when A requests message M as a signature, B looks up $(M_i, \sigma_i, y_i, c_i)$ in the list query such that $M_i = M$.

If $c_i \neq 0$, we return σ_i.

Otherwise, $c_i = 0$, interrupts.

(4) Output: A outputs (M, σ). B looks for M in the query list corresponding to the quadruple $(M_i, \sigma_i, y_i, c_i)$, if $c_i \neq 0$, B interrupts.

In the above reduction process, c_i is the guess of B. $c_i = 0$ corresponding to the message that M in the quadruple is the signature that A will eventually forge and the role of c_i in the quadruple $(M_i, \sigma_i, y_i, c_i)$ is an identifier.

The success of B is determined by the following three events:

π_1: B does not break in A 's signature query

π_2: A produces a valid message-signature pair (M, σ)

π_3: π_2 occurs and c is equal to 0 in the quadruplet (M, σ, y, c) corresponding to M.

$\Pr[\pi_1] = (1 - \delta)^{q_s}$, $\Pr[\pi_2|\pi_1] = \varepsilon(K)$, and $\Pr[\pi_3|\pi_2\pi_1] = \Pr[0|\pi_2\pi_1] = \delta$. So, the success rate of B is $\Pr[\pi_3\pi_1] = \Pr[\pi_1] \cdot \Pr[\pi_2|\pi_1] \cdot \Pr[\pi_3|\pi_2\pi_1] = (1 - \delta)^{q_s} \in \delta$.

Considering $(1 - \delta)^{q_s} \in \delta$ as a function of δ, when $\delta = 1/q_s + 1$ can be obtained, $(1 - \delta)^{q_s} \in \delta$ reaches the maximum, and the maximum value is $\varepsilon(k)/e(q_s + 1) \approx \varepsilon(k)/e(q_s)$. The proof is complete.

Compared to previous pair schemes, our scheme has a larger pair advantage in terms of efficiency, since all messages are encoded as low-dimensional matrices, and the scaling rate in terms of storage and computational overhead is linear compared to plaintext implementations. Horan K. et al. [33] mentioned that the CSP problem is in a general linear group $GL_d(R)$ (where R represents the real number field); if $d > 4$, CSP can be proved to be anti-quantum secure, so when we encode the message M as a matrix, it is necessary to keep its dimension greater than 4. Specifically, we assume that G is a general noncommutative semigroup, $a \in G^{-1}$ and $b \in G$, and the function $F_a(M)$ can be regarded as a pair of preprocessing for the message M. For any message M originating from the real domain R, we can encode $b^{|M|}$ as a 6-dimensional upper triangular matrix, denoted by $M \in R^{6\times 6}$.

We use three pairs of random numbers (m_1, m_2), (m_3, m_4), (m_5, m_6) to represent the message M, while satisfying certain properties: $m_1 + m_2 = M, m_3 + m_4 =$

$m_5 + m_6 = r$, where r is a system random number. With these elements, we construct the matrix as follows:

$$M_1 = \begin{pmatrix} m_1 & m_2 \\ m_2 & m_1 \end{pmatrix},$$
$$M_2 = \begin{pmatrix} m_3 & m_4 \\ m_4 & m_3 \end{pmatrix}, \tag{28}$$
$$M_3 = \begin{pmatrix} m_5 & m_6 \\ m_6 & m_5 \end{pmatrix}.$$

Combining the above three small matrices, the final encoding form of the message M is as follows:

$$M = \begin{pmatrix} M_1 & R_1 & R_2 \\ 0 & M_2 & R_3 \\ 0 & 0 & M_3 \end{pmatrix}. \tag{29}$$

0 here also represents an all-zero matrix of 2×2. R_i $(i = 1, 2, 3)$ represents a random matrix uniformly sampled from the real number domain $R^{2\times 2}$.

Next, we perform the encoding operation on a. We uniformly randomly sample a matrix from $R^{6\times 6}$ to represent a, which can also be considered as 9 random matrices of 2×2, as expressed in the following form:

$$a = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}, \text{for } a_i = \begin{pmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4} \end{pmatrix}, (i = 1, 2, \ldots, 9). \tag{30}$$

The probability that message space M communicates with elements in a is negligible. It can be understood in this way that a here is similar to a key for encrypting a message M, so there are the following operations:

$$H = F_a(M) = aMa^{-1} = a\begin{pmatrix} M_1 & R_1 & R_2 \\ 0 & M_2 & R_3 \\ 0 & 0 & M_3 \end{pmatrix}a^{-1}, \tag{31}$$

where H is the input parameter for the subsequent execution of the RSA algorithm, which can also be regarded as the encryption of the message M, where a can be understood as a symmetric key. In some specific cases, we can perform conflict tracking, use a to solve H, recover the message from M_1, and recover the signer pair identity from M_2 (assuming the user identity information is placed in it).

The security (antiforgery) of $F_a(M) = aMa^{-1}$ proves the following.

First, we carry out the following operations:

$$\det(H^* - TH') = \det(a)\det\left(\begin{pmatrix} M_1^* - TM_1' & R_1^* & R_2^* \\ 0 & M_2^* - TM_2' & R_3^* \\ 0 & 0 & M_3^* - TM_3' \end{pmatrix}\right)\det\left(a^{-1}\right), \tag{32}$$

where R_i^*, $(i = 1, 2, 3)$ are random matrices. The representation of T is as follows:

$$T = \begin{pmatrix} t & R_1 & R_2 \\ 0 & t & R_3 \\ 0 & 0 & t \end{pmatrix}, \tag{33}$$

among them

$$t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{34}$$

R_i, $(i = 1, 2, 3)$ is randomly sampled from $R^{2\times 2}$. The adversary is defined to launch a forgery attack according to the following algorithm, which is formally described as follows [34]:

$$\begin{aligned}
&\mathrm{Exp}_{\pi,A}^{\mathrm{CPA}}(K):\\
&(k)\leftarrow \mathrm{KeyGen}(K),\\
&(M_0, M_1, H)\leftarrow A^{F_k(\cdot)}, \text{there}\left|M_0\right| = \left|M_1\right|,\\
&H' = F_k(H), \text{and } M_0 < H < M_1,\\
&\beta\leftarrow R_{\{0,1\}}, H^* = \varepsilon_k\left(M_\beta\right),\\
&\beta' = 1, if \det\left(H^* - TH'\right), \beta' = 0, \text{otherwise},\\
&\text{Output } 1, if \beta = \beta', \text{Output } 0, \text{otherwise}.
\end{aligned} \tag{35}$$

The adversary's advantage is defined as follows:

$$\mathrm{Adv}_{\pi,A}^{\mathrm{CPA}}(K) = \left|\Pr\left[\mathrm{Exp}_{\pi,A}^{\mathrm{CPA}}(K) = 1\right] - \frac{1}{2}\right|. \tag{36}$$

We will try to expand the content of the if conditional statement $\det(H^* - TH')$:

$$\det\left(H^* - TH'\right) = \det(p)\det\left(M_i^* - tM_i'\right)\det\left(p^{-1}\right), (i = 1, 2, 3), \tag{37}$$

among them

$$\det\left(M_i^* - tM_i'\right) = \left(a_{2i-1}^* - a_{2i}'\right)^2 - \left(a_{2i}^* - a_{2i-1}'\right)^2 = \left(m^* - m'\right)\left(\left(a_{2i-1}^* - a_{2i}^*\right)t - \left(a_{2i}' - a_{2i-1}'\right)n\right). \tag{38}$$

However, by borrowing the scheme of Li et al. [35], we can clarify $a_{2i-1} > a_{2i}$. So, the part of $((a_{2i-1}^* - a_{2i}^*)t - (a_{2i}' - a_{2i-1}')n)$ always satisfies positive, and $\det(p)\det(p^{-1}) = 1$. Therefore, for an attacking adversary, to distinguish whether the signed message is M_0 or M_1, he only needs to calculate $\det(H^* - TH')$ according to the sign of the returned value. If a positive value is returned, 1 is output, representing the guessed signature message as $M^* = M_1$. If a negative value is returned, 0 is output, which means the guessed signature message is $M^* = M_0$. Therefore, the advantage of the adversary is 1, which means that the scheme is not anticounterfeiting.

The advantage of our proposed scheme is that we are a probabilistic encryption scheme. There can be multiple encoding forms for m'. First, a random even number ρ is selected to encrypt m', and the following form is obtained:

$$\begin{aligned}
H' &= F_a\left(M'^{\rho}\right) = aM'^{\rho}a^{-1}\\
&= a\begin{pmatrix} M_1^{\rho} & R_1 & R_2\\ 0 & M_2^{\rho} & R_3\\ 0 & 0 & M_3^{\rho}\end{pmatrix}a^{-1} = F_a^{\rho}(M').
\end{aligned} \tag{39}$$

According to the properties $F_a(b^m) = F_a^m(b)$ of the CSP-LD system, we mentioned earlier, and the upper triangular matrix encoding form of M is

$$M = \begin{pmatrix} M_1 & R_1 & R_2\\ 0 & M_2 & R_3\\ 0 & 0 & M_3\end{pmatrix}. \tag{40}$$

We can infer

$$\left|M^{\rho}\right| = |M|^{\rho}, (i = 1, 2, 3). \tag{41}$$

Therefore,

$$\begin{aligned}
\det\left(H^* - TH'\right) &= \det(p)\det\left(M_i^* - tM_i'\right)^{\rho}\det\left(p^{-1}\right), (i = 1, 2, 3) = \det\left(M_i^* - tM_i'\right)^{\rho},\\
&= \left(m^* - m'\right)^{\rho}\left(\left(a_{2i-1}^* - a_{2i}^*\right)t - \left(a_{2i}' - a_{2i-1}'\right)n\right)^{\rho}.
\end{aligned} \tag{42}$$

Because ρ is an even number, the adversary always has a positive value when calculating $\det(H^* - TH')$, and it is impossible to determine whether the signature comes from M_0 or M_1. □

5. RSA-like Aggregate Signature Scheme Based on CSP-LD System

Before formally introducing the aggregate signature scheme, we need to make a formal specification of the paired element in G for a secure and valid pair.

Specification 1: in a CSP-LD system, the representation of elements in G is unique

Specification 2: it is possible to efficiently convert an element in G to its regular form

Specification 3: the length of $F_{a^t}(b)$ does not show any information about a^t.

According to Definition 3, we suppose a and b are random numbers, $a \in G^{-1}$ and $b \in G$, which are given and fixed for the system parameters, and we assume that G is a general noncommutative semigroup, and the binary function F satisfies the following conjugation operations:

$$F\colon G^{-1} \times G \longrightarrow G, \quad (a,b) \longrightarrow aba^{-1}. \tag{43}$$

We denote $F(a,b) = aba^{-1}$ as $F_a(b)$.

Assuming that there are different users $p_1, p_2, \ldots, p_N$, in a multiuser environment, the message M needs to be co-signed. Our RSA aggregate signature scheme based on the CSP-LD system consists of the following algorithms.

(1–1) message encoding: the message M is composed of $m_{i\,(i=1,2,\ldots,6)}$ satisfying some certain property, $m_1 + m_2 = M$ and $m_3 + m_4 = m_5 + m_6 = r$, where r is a system random number, and an even number ρ is sampled from the random number in the real number domain. We construct the matrix as follows:

$$M_i^\rho = \begin{pmatrix} m^\rho_{(2*i)-1} & m^\rho_{2*i} \\ m^\rho_{2*i} & m^\rho_{(2*i)-1} \end{pmatrix}, (i = 1,2,3). \tag{44}$$

Combining the above three submatrices, the final encoding form of the message M is as follows:

$$M^\rho = \begin{pmatrix} M_1^\rho & R_1^\rho & R_2^\rho \\ 0 & M_2^\rho & R_3^\rho \\ 0 & 0 & M_3^\rho \end{pmatrix}. \tag{45}$$

0 here also represents an all-zero matrix of 2×2. $R_i\,(i = 1,2,3)$ represents a random matrix uniformly sampled from the real number domain $R^{2\times 2}$.

(1–2) coding form of a: we uniformly randomly sample a matrix from $R^{6\times 6}$ for encoding, representing a, which can also be considered as 9 random matrices of 2×2, expressed in the following form:

$$a = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}, \text{for } a_i = \begin{pmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4} \end{pmatrix}, (i = 1,2,\ldots,9). \tag{46}$$

(1) Key generation is as follows:

$$\begin{aligned} &\text{GenRSA}(k): \\ &s_{i,(i=1,2,\ldots,N)}, p, q \leftarrow \text{GenPrime}(k), \\ &N = pq, \varphi(n) = (p-1)(q-1), \\ &\text{Take } e, \text{satisfying } 1 < e < j(n) \text{and} (j(n), e) = 1, \\ &\text{Compute } d, \text{satisfying } d \cdot e \equiv 1 \bmod \varphi(n), \\ &\text{Calculate } w, w = \sum_{i=1}^{N} s_i, \\ &pk = (n, e, w), sk = (n, d, s_i). \end{aligned} \tag{47}$$

(2) Signature is as follows:

$$\begin{aligned} &\text{Sign}_{sk}(M): \\ &H = \sum_{i=1}^{N} F^\rho_{a^{s_i}}(M), \\ &\sigma = H^d \bmod n. \end{aligned} \tag{48}$$

(3) Verify is as follows:

$$\text{Vrfy}_{pk}(M, \sigma). \tag{49}$$

If $\sigma^e = F^\rho_{a^w}(M) \bmod n$, we return 1; otherwise, we return 0.

Proof of the correctness of the scheme: according to Lemma 2, the CSP-LD system satisfies the following properties:

$$\begin{aligned} F_{a^m}(b) &= a^m b a^{-m} = a^s a^t b a^{-t} a^{-s} \\ &= a^s F_{a^t}(b) a^{-s} = F_{a^s}(F_{a^t}(b)). \end{aligned} \tag{50}$$

Because of $w = \sum_{i=1}^{3} s_i$, we get $\prod_{i=1}^{3} F^\rho_{a^{s_i}}(M) = F^\rho_{a^w}(M)$. On the question of whether the security is satisfied, we can infer from the previous point that since M is an upper triangular matrix, it satisfies

$$\left|M^\rho\right| = |M|^\rho, (i = 1,2,3). \tag{51}$$

When the adversary tries to distinguish M_0 or M_1 by computing the determinant,

$$\begin{aligned} \det(H^* - TH') &= \det(p)\det(M_i^* - tM_i')^\rho \det\left(p^{-1}\right), (i = 1,2,3) = \det(M_i^* - tM_i')^\rho \\ &= (m^* - m')^\rho \left((a^*_{2i-1} - a^*_{2i})t - (a'_{2i} - a'_{2i-1})n\right)^\rho. \end{aligned} \tag{52}$$

Table 1: The efficiency comparison between our scheme and literature [24, 36].

	Assumption	Signature length	Signature algorithm	Verification algorithm	Saving rate
Literature 24	Pairing	320	$2nE + nH$	$nH + (3n-1)P$	50%
Literature 36	RSA	160	nE	$(n+1)E$	50%
Our scheme	RSA	160	nE	$2E$	Fixed length

Table 2: The security comparison between our scheme and [3, 6, 24].

	EUF-CMA	Antiquantum security
Literature 24	No	No
Literature 36	Yes	No
Our scheme	Yes	Yes

Table 3: Notations.

Notations	Description
k	The system parameters
p, q	Two large prime numbers are chosen at random
pk, sk	The public key and private key
σ	Result of signing the message
$F_a(b)$	Functions satisfying certain properties under the CSP-LD system
G	A general noncommutative semigroup
p_i	Users
M	Message
$m_{i(i=1,2,\ldots,6)}$	They together according to certain rules to form a message M
r	Random number
ρ	Random even number
a	9 random matrices of 2×2
$(M_i, \sigma_i, y_i, c_i)$	The quadruple, σ_i, is the signature of M_i, y_i is the query result of an adversary A to M_i, and c_i is a random value of 0 1
s_i	User ID number
w	The sum of all s_i
t	Special 0 and 1 matrix
R_i, $(i = 1, 2, 3)$	The randomly sampled matrices from $R^{2\times 2}$
T	The upper triangular encoding matrix
H	Regarded as the encryption of the message M under the function F

Because the value of ρ is an even number (it can be set to $\rho = 2$), the adversary cannot determine whether the signature comes from M_0 or M_1 based on the value calculated by $\det(H^* - TH')$, so H satisfies the selection of plaintext antiforgery. According to the previous inference in Definition 4, the aggregated signature scheme proposed by us is still antiforgery under the adaptive chosen message attack.

According to the algorithm proposed by Shor, a quantum computer with N qubits can perform 2^N operations at a time. In theory, the key is the 1024 bit long RSA algorithm, which can be cracked in 1 second with a 512 bit quantum computer. At present, as long as the proposed scheme is set s_i to a 160 bit integer, it can resist the exhaustion-resistant attack [27].

6. Efficiency Analysis

Now, we compare the computational efficiency of the RSA aggregate signature scheme under the CSP-LD system with some other aggregate signature schemes. Still assume that there are N users signing messages M at the same time. For each signature, if the aggregation method is not used, the original RSA signature method without aggregation method needs to store a total of N pairs of $(M, \sigma_1), \ldots, (M, \sigma_N)$ signatures. While the scheme in [36] improves the efficiency by 50%, the signature they store is $(M, \sigma_1, \ldots, \sigma_N)$. In our scheme, no matter how many users there are, we only need to store a pair of signatures, namely, (M, σ), which benefits from the advantages of the CSP-LD system. Compared with [36], our improved efficiency has a linear relationship with the value of N, and the larger the value, the greater the advantage of our scheme. Compared with the pairing-based scheme in [24], our advantage is even more obvious, since it is known that a pairing operation takes approximately 6–20 times the time of a modulo-exponential operation [25].

In addition, since all messages are encoded as low-dimensional matrices, the scaling rate in terms of storage and computation overhead is linear compared to message signature implementations and the length of aggregated signatures is fixed, maximizing signature storage savings space without losing accuracy. In terms of security, our scheme is also indestructible to a large extent, and the strongest attack method against the signature scheme, the adaptive chosen message attack, is still existentially unforgeable. Moreover,

by setting the system parameter thresholds on the matrix dimension and the length of the private key, antiquantum attacks, and exhaustive attacks can be achieved.

Explanation of symbols in Table 1: Exp represents a power of 1 operation, H represents a hash operation, P represents a bilinear pairing operation, and n represents the number of users. Assuming that the following three schemes all select the group G whose order is the same prime number q, if the system parameter k is 160 bits, the length of the group G is calculated as $|G| = 160$bit. The details are shown in Table 1.

The details of the security comparison between our scheme and literature are shown in Table 2.

7. Conclusion

This study improves the RSA-like signature scheme by proposing new schemes that take advantage of CSP-LD systems to encode messages with the low-dimensional matrix. By flexibly changing the encoding structure, it can perfectly satisfy the antiforgery under the adaptive choice message attack (EUF-CMA) without using the global hash function. Setting the matrix dimension greater than the critical value can achieve the antiquantum attack, and controlling the length of the user's s_i element longer than a certain bit can resist exhaustive attacks. In the environment where N users sign a message, we implement the aggregated signature under the RSA structure according to the CSP-LD system, which greatly reduces the generation of public and private key pairs. Moreover, the final signature pair has nothing to do with the number of users, which saves a lot of storage space and improves computing efficiency. In the future, we look forward to combining the signature scheme with cutting-edge technologies such as blockchain technology, smart contracts [37], and machine learning [38] to improve the deployment of the scheme, learn from each other's strengths, and furthermore, improve efficiency and security.

7.1. The notations of this work. In this section, we explain all the specific characters in the study; the details are shown in Table 3.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the "Chengdu-Chongqing Economic Circle Construction" Scientific and Technological Innovation Project of Chongqing Municipal Education Commission, under Grant KJCX2020033, the National Natural Science Foundation of P.R., China, under Grants 61903053 and 62273065, the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, under Grant AGK2020006, and the Chongqing Municipal Education Commission Research Program, under Grants KJQN201900702 and KJZD-K201800701.

References

[1] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press LLC, Second Edition, 2002.

[2] A. J. Menezs, P. C. V. Oorchot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[3] B. Schneier, *Applied Cryptography. Protocols, Algorithms and Source in C*, John Wiley & Sons, Second Edition, 1995.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the International conference on the theory and applications of cryptographic techniques*, pp. 416–432, Springer, Berlin, Heidelberg, May 2003.

[6] K. Hashimoto and W. Ogata, "Unrestricted and compact certificateless aggregate signature scheme," *Information Sciences*, vol. 487, no. 1, pp. 97–114, 2019.

[7] T. Iwasaki, N. Yanai, M. Inamura, and K. Inamura, "Tightly-secure identity-based structured aggregate signature scheme under the computational diffie-hellman assumption," in *Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications*, pp. 669–679, IEEE, Crans-Montana, Switzerland, March 2016.

[8] A. Boldyreva, C. Gentry, and A. O'Neill, "Ordered multi-signatures and identity-based sequential aggregate signatures, with applications to secure routing," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 276–285, ACM, Alexandria, Egypt, January 2007.

[9] Z. Shao, "On the sequentiality of three optimal structured multisignature schemes," in *Proceedings of the International Conference on Information Security Practice and Experience*, pp. 105–115, Springer, Berlin, Heidelberg, 2007.

[10] Z. Guan, N. Wang, X. Fan, X. Liu, L. Wu, and S. Wan, "Achieving secure search over encrypted data for e-commerce: a blockchain approach," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–17, 2021.

[11] L. Zhao, M. B. Saif, A. Hawbani, G. Min, S. Peng, and N. Lin, "A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET," *China Communications*, vol. 18, no. 7, pp. 103–116, 2021.

[12] Y. Liu, W. Yu, Z. Ai, G. Xu, L. Zhao, and Z. Tian, "A blockchain-empowered federated learning in healthcare-based cyber physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 6, pp. 4482–4494, 2022.

[13] C. Wang, X. Wu, G. Liu, T. Deng, K. Peng, and S. Wan, "Safeguarding cross-silo federated learning with local differential privacy," *Digital Communications and Networks*, vol. 8, pp. 446–454, 2021.

[14] L. Zhao, H. Li, N. Lin, M. Lin, C. Fan, and J. Shi, "Intelligent content caching strategy in autonomous driving toward 6G," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9786–9796, 2022.

[15] S. Wan, "Topology hiding routing based on learning with errors," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 14, pp. 1–10, 2020.

[16] L. Zhao, C. Wang, K. Zhao, D. Tarchi, S. Wan, and N. Kumar, "INTERLINK: A digital twin-assisted storage strategy for satellite-terrestrial networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 5, pp. 3746–3759, 2022.

[17] S. Mao, L. Liu, N. Zhang et al., "Reconfigurable intelligent surface-assisted secure mobile edge computing networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6647–6660, 2022.

[18] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max Cost Optimization for efficient hierarchical federated learning in Wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 1–2700, 2022.

[19] L. Zhao, Z. Bi, A. Hawbani, K. Yu, Y. Zhang, and M. Guizani, "ELITE: An intelligent digital twin-based hierarchical routing scheme for softwarized vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 12, pp. 4667–4685, 2022.

[20] L. Zhao, Z. Li, A. Y. Al-Dubai et al., "A novel prediction-based temporal graph routing algorithm for software-defined vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 13275–13290, 2022.

[21] L. Zhao, T. Zheng, M. Lin, A. Hawbani, J. Shang, and C. Fan, "SPIDER: A social computing inspired predictive routing scheme for softwarized vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9466–9477, 2022.

[22] Y. P. Li, H. H. Nie, and Y. W. Zhou, "A novel and provably secure certificateless aggregate signature scheme," *Journal of Cryptologic Research*, vol. 2, no. 6, pp. 526–535, 2015.

[23] Y. W. Zhou, B. Yang, and W. Z. Zhang, "Efficient and provide security certificateless aggregate signature scheme," *Journal of Software*, vol. 26, no. 12, pp. 3204–3214, 2015.

[24] X. D. Yang, X. Z. Pei, and F. Y. An, "Message authentication scheme for vehicular ad hoc network using identity-based aggregate signature," *Computer Engineering*, vol. 46, no. 2, pp. 170–174+182, 2020.

[25] M. Bellare and G. Neven, "Identity-based multi-signatures from RSA," *Cryptographers' Track at the RSA Conference*, pp. 145–162, Springer, Berlin, Heidelberg, 2007.

[26] J. Buchmann, C. Coronado, M. Döring et al., *Post-quantum Signatures*, Cryptology ePrint Archive, 2004.

[27] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[28] P. Dehornoy, "Using shifted conjugacy in braid-based cryptography," *Contemporary Mathematics*, vol. 418, no. 9, pp. 65–74, 2006.

[29] L. Wang, L. Wang, and Z. Cao, "New constructions of public-key encryption schemes from conjugacy search problems," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 1–17, Springer, Berlin, Heidelberg, 2010.

[30] S. Goldwasser, S. Micali, and R. L. Rivest, "A paradoxical solution to the signature problem," *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, 2019.

[31] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[32] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Annual International Cryptology Conference*, pp. 41–55, Springer, Berlin, Heidelberg, 2004.

[33] K. Horan and D. Kahrobaei, "The hidden subgroup problem and post-quantum group-based cryptography," in *International Congress on Mathematical Software*, pp. 218–226, Springer, Cham, 2018.

[34] F. T. Kuang, B. Mi, Y. Li, Y. Weng, and S. Wu, "Multiparty homomorphic machine learning with data security and model preservation," *Mathematical Problems in Engineering*, vol. 2021, Article ID 6615839, 8 pages, 2021.

[35] J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes," *Information Sciences*, vol. 526, no. 1, pp. 166–179, 2020.

[36] B. Dou, C. H. Chen, H. Zhang, and C. Xu, "Identity-based sequential aggregate signature scheme based on RSA," *International journal of innovative computing information and control*, vol. 8, no. 9, pp. 6401–6413, 2012.

[37] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K. K. R. Choo, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12004–12020, 2021.

[38] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis et al., "Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2041–2052, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5094830, 12 pages
https://doi.org/10.1155/2022/5094830

Research Article

Privacy-Preserving Vertical Collaborative Logistic Regression without Trusted Third-Party Coordinator

Xiaopeng Yu,[1] **Wei Zhao**,[1] **Dianhua Tang**,[1,2] **and Kai Liang**[3]

[1]*Science and Technology on Communication Security Laboratory, Chengdu 610041, China*
[2]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*
[3]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Dianhua Tang; tangdianhua86@163.com

Received 28 July 2022; Accepted 13 September 2022; Published 12 October 2022

Academic Editor: Jianbo Du

Collaborative learning is an emerging distributed learning paradigm, which enables multiple parties to jointly train a shared machine learning (ML) model without causing the disclosure of the raw data of each party. As one of the fundamental collaborative learning algorithms, privacy-preserving collaborative logistic regression has recently gained attention from industry and academia, which utilizes cryptographic techniques to securely train joint logistic regression models across data from multiple parties. However, existing schemes have high communication and computational overhead, lose the ability to deal with high-dimensional sparse samples, cut down the accuracy of the model, or exist the risk of leaking private information. To overcome these issues, considering vertically distributed data, we propose a privacy-preserving vertical collaborative logistic regression (P^2VCLR) based on approximate homomorphic encryption (HE), which enables two parties to jointly train a shared model without a trusted third-party coordinator. Our scheme utilizes batching method in approximate HE to encrypt multiple data into a single ciphertext and enable a parallel processing through single instruction multiple data (SIMD) manner. We evaluate our scheme by using three publicly available datasets, the experimental results indicate that our scheme outperforms existing schemes in terms of training time and model performance.

1. Introduction

Machine learning (ML) [1] is a method for analyzing large-scale data and is widely used in practice to train predictive models for practical applications. As one of the basic machine learning algorithms, logistic regression (LR) [2] has attracted much attention for its powerful ability to solve classification problems in practical applications, such as disease diagnosis [3], credit evaluation [4].

In recent years, in order to obtain massive data for training better-performing models [5], there is growing interest in machine learning by combining the data from different institutions [6]. For instance, different hospitals would like to combine health data to jointly train models to facilitate more accurate disease diagnosis; different financial companies want to collaborate to train more effective credit card scoring and fraud detection models. Unfortunately, due to regulatory and competitive reasons, it is difficult or even impossible to directly exchange data of different parties for model training in practice [7]. That is, the data of different organizations is isolated. To eliminate the issue of "data isolation", the idea of collaborative learning [8] is introduced. Its goal is to cooperatively train a shared ML model on distributed data while complying with regulation and protecting privacy. The security, privacy, and efficiency concerns remain main challenges for practical applications. Recently, as a fundamental collaborative learning algorithm, privacy-preserving collaborative logistic regression (PPCLR) [9–24] has received considerable attention recently, which utilizes cryptographic primitives such as homomorphic encryption (HE) algorithm [25] and multi-party computation (MPC) protocol [26] to securely train a joint logistic regression model across data from multiple parties. However, for the HE-based schemes [9–11], model weights are

exposed to all parties at each iterative update of global model parameters during training, which is able to be utilized to deduce additional private information [27]; for the MPC-based schemes [12, 14], after using secret sharing (SS) [28] on training samples of all parties, even previously sparse samples become dense, so they are not able to efficiently handle sparse samples and require high communication complexity when the training data becomes large.

To solve the problems mentioned above, in a two-party setting, considering two vertically distributed training data with the same sample distributions but different feature distributions, we construct a privacy-preserving vertical collaborative logistic regression (P^2 VCLR) based on the HE for arithmetic of approximate numbers [29]. The main contributions are as follows:

(1) Firstly, we construct a P^2 VCLR framework for collaborative learning of vertical distributed features, which can securely realize the joint modeling of both parties without the assistance of a trusted third-party (TTP), and hence greatly reduces the system complexity.

(2) Secondly, to improve the training efficiency, using the batching technique in HE [29], the proposed scheme can pack multiple samples into a single plaintext with multiple slots, encrypt it into a single ciphertext, and enable a parallel computing through using SIMD.

(3) Finally, we conduct performance evaluations on three datasets [30], and the experimental evaluation results indicate that our scheme achieves a significant improvement in efficiency and performance than existing schemes [9, 21]. Specifically, the training time of the model is decreased by almost 32.3%-72.5%; the accuracy, F1-score, and AUC of the model have nearly 0.3% - 3.0%, 0.1% - 2.7% and 0 - 0.03 improvement, respectively. Furthermore, the security analysis indicates that the proposed P^2 VCLR scheme is secure against semi-honest adversaries, and neither of the both parties can know each other's raw data.

The rest of this work is arranged as follows. Several works related to our scheme are introduced in Section [2]. In Section [3], we review some preliminaries. In Section [4], our scheme is described. In Section [5], the evaluations for our scheme are presented. The security analysis of our scheme is shown in Section [6]. In Section [7], we conclude this work.

2. Related Works

There are several works that have been made to joint train a LR model across multiple data owners. In general, a common approach is to implement secure logistic regression by using cryptographic primitives like HE [25] and MPC [26]. The existing works [9–24] can be divided into two categories: PPCLR with a TTP coordinator [9–16] and PPCLR without a TTP coordinator [17–24]. A summary of the existing works [9–24] follows.

As for the PPCLR with TTP coordinator [9–16], Hardy *et al.* [9] described a privacy-preserving federated LR scheme by employing additively HE scheme [25], which centralizes two vertically distributed training data in one TTP coordinator, but the approximation of non-polynomial function reduces the model accuracy. Yang *et al.* [10] shown a quasi-Newton way for achieving vertical federated LR model based on the additively HE scheme [25]. Using an additive HE [31] and an aggregation method [32], Mandal *et al.* [11] built a privacy-preserving regression analysis protocol on the horizontally distributed high-dimensional data. Employing an additive secret sharing technique [33], Zhang *et al.* [12] proposed a privacy-preservation collaborative learning for ensuring local training data and model information. Liu *et al.* [13] introduced a collaborative learning platform, which supports multiple institutions to build machine learning models collaboratively over large-scale horizontally and vertically partitioned data. By means of MPC from additive secret sharing [34, 35], Cock *et al.* [14] proposed a protocol for securely training LR model over distributed parties, where TTP initializer assigns relevant random values to two computing severs. Based on multi-key fully HE [36], Wang *et al.* [15] designed a secure cloud-edge collaborative LR system, which employs the cloud centre and edge nodes to collaboratively train a LR model over encrypted data. Zhu *et al.* [16] proposed a value-blind LR training method in a collaborative setting based on HE [25], where the central server updates model parameters without access to the training data and intermediate values, and model parameters are shared among the central server with collaborating parties. However, it's inherently difficult to establish a third party trusted by any data owners in a real-world scenario. Moreover, data interactions between data owners and TTP raise the risk of leakage of sensitive data of the data owner.

To decrease the complexity of training a joint model for any two parties, by removing the TTP coordinator, Yang *et al.* [17] constructed a parallel distributed LR method for vertical federated learning based on HE [25], which allows two parties to jointly train models without the help of a TTP coordinator. Using the secure MPC protocol and ciphertext domain conversion protocol [37], Chen *et al.* [18] presented a collaborative learning system for jointly building better models over vertically partitioned multiple data. Based on the HE scheme [29], Li *et al.* [19] introduced a collaborative learning method on encrypted data, which could securely train LR models over vertically distributed data from both data owners. Based on asynchronous gradient sharing and HE algorithm [29], Wei *et al.* [20] designed a two-parties collaborative LR protocol, which can train securely joint model on the vertically partitioned data. Chen *et al.* [21] combined the HE [25] and secret sharing [38] to build securely LR model on the vertically distributed large-scale sparse training data. Over the horizontally partitioned data, based on secure MPC protocol, Ghavamipour *et al.* [22] described two methods to train LR model in a privacy-preserving manner. However, each data owner requires to compute multiple shares of its sensitive training data and sends them separately to each non-collusion computation party, this leads to heavy communication costs. He *et al.* [23]

constructed a vertical federated LR method through a HE algorithm [25], which uses a piecewise function to ensure the accuracy of the loss function, but this results in a loss of efficiency. With the HE scheme [25] and differential privacy algorithm [39], Sun *et al.* [24] introduced a vertical federated LR solution, which alleviates the constraints on feature dimensions. However, the existing PPCLR schemes [17–24] without a TTP coordinator lead to high communication and computational overhead.

3. Preliminaries

3.1. System Architecture. For ease of reading, the definitions of the symbols in our P^2 VCLR scheme are displayed in Table 1. As is shown in Figure 1, the system architecture of our P^2 VCLR includes two semi-trusted entities: P_a and P_b. P_a and P_b hold the vertically distributed datasets S_a and S_b, respectively. S_a and S_b have the same sample space but different feature distribution, namely, P_a holds the part of the features, P_b holds another part of the features and the label. P_a cooperates with P_b to train a shared LR model without disclosing the privacy of training data. Specifically, P_a generates $\{sk_a, pk_a, rk_a, gk_a\} \leftarrow \mathrm{KeyGen}(N, Q)$ [29], sends polynomial-degree N, coefficient-modulus Q, scaling factor Δ, public key pk_a, relinearization key rk_a, galois key gk_a to P_b, and securely store secret key sk_a. Then, P_a encrypts its own data with pk_a, and sends the encrypted data to P_b. Finally, P_a and P_b jointly execute P^2 VCLR algorithm to obtain the training result.

3.2. Homomorphic Encryption. HE allows direct operations on ciphertext without decryption, and can ensure that the computation on the ciphertext is consistent with the computation on the plaintext. Cheon *et al.* [29] introduced an approximate HE algorithm from ring learning with errors (RLWE) [40], which supports the following operations.

(1) $\{sk_i, pk_i, rk_i, gk_i\} \leftarrow \mathrm{Key\_Gen}(N, Q)$: Given the parameters $\{N, Q\}$, it generates sk_i, pk_i, rk_i, gk_i for P_i.

(2) $x \leftarrow \mathrm{Enc}(x, pk_i)$: Given a message vector x and pk_i, it generates a ciphertext x.

(3) $x \leftarrow \mathrm{Dec}(x, sk_i)$: Given x and sk_i, it generates a message vector x.

(4) $x + y \leftarrow \mathrm{Add}(x, y)$: Given x and y, it generates a ciphertext $x + y = x + y$.

(5) $x + y \leftarrow \mathrm{Add\_Plain}(x, y)$: Given x and a message vector y, it generates a ciphertext $x + y = x + y$.

(6) $x_0 + \cdots + x_{n-1} \leftarrow \mathrm{Add\_Many}(x, y)$: Given a ciphertext list $X = \{x_0, \ldots, x_{n-1}\}$, it generates a ciphertext $x_0 + \cdots + x_{n-1} = x_0 + \cdots + x_{n-1}$.

(7) $x - y \leftarrow \mathrm{Sub}(x, y)$: Given x and y, it generates a ciphertext $x - y = x - y$.

(8) $x - y \leftarrow \mathrm{Sub\_Plain}(x, y)$: Given x and y, it generates a ciphertext $x - y = x - y$.

(9) $x * y \leftarrow \mathrm{Mul}(x, y, rk_i)$: Given x, y and rk_i, it generates a ciphertext $x * y = x * y$.

(10) $x * y \leftarrow \mathrm{Mul\_Plain}(x, y, rk_i)$: Given x, y and rk_i, it generates a ciphertext $x * y = x * y$.

(11) $y \leftarrow \mathrm{Rot\_Vector}(x, k, gk_i)$: Given $x = [x_0, \ldots, x_{N/2-1}]$, k and gk_i, it rotates x left by rotation value k, and generates a ciphertext $y = [x_k, \ldots, x_{N/2-1}, x_0, \ldots, x_{k-1}]$.

3.3. Logistic Regression. Let a dataset S includes m samples $\{x_{i,1}, \ldots, x_{i,n}, y_i | i \in [m]\} = \{x_i, y_i | i \in [m]\}$, where an input x_i maps to a binary dependent variable $y_i \in \{0, 1\}$, the goal of binary LR is to compute weights $\xi = \{\xi_0, \xi_1, \ldots, \xi_n\}$ that minimizes the log-likelihood loss function $J(\xi) = -1/m \cdot \sum_{i=1}^{m} ((1 - y_i) \cdot (1 - \log(\sigma(z_i \cdot \xi))) + y_i \cdot \log(\sigma\ (z_i \cdot \xi)))$, where $z_i = \{1, x_i\}$. Assuming that $\xi^{(k)}$ and $\alpha^{(k)}$ denote the model weights and learning rate at iteration k, respectively, the gradient descent (GD) is able to be used to compute the extremum of $J(\xi)$ by $\xi^{(k+1)} \leftarrow \xi^{(k)} - \alpha^k/m \cdot \sum_{i=1}^{m} ((\sigma(z_i \cdot \xi^{(k)}) - y_i) \cdot z_i)$. Since the HE scheme (CKKS) [29] is not able to effectively support non-polynomial arithmetic operations, we use a 7-degree polynomial function $f(x) = w_0 + w_1 x + w_3 x^3 + w_5 x^5 + w_7 x^7$ to approximate sigmoid function $\sigma(x) = 1/(1 + e^{-x})$ over the domain [-8, 8], where $w_0 = 1/2$, $w_1 = 1.73496/8$, $w_3 = 4.19407/8^3$, $w_5 = 5.43402/8^5$, and $w_7 = 2.50739/8^7$.

4. Privacy-Preserving Vertical Collaborative Logistic Regression

Over vertically distributed datasets S_a and S_b, we propose a P^2 VCLR scheme based on an approximate HE [29]. Using batching method in approximate HE, the proposed scheme packs a message vector with multiple messages into a plaintext with multiple plaintext slots, and performs parallel training based on SIMD. For ease of readability, we give the Algorithm , which can be found in Appendix. We assume that the samples of S_a and S_b held by P_a and P_b have been aligned, namely,

Table 1: The definition of the symbol.

Notation	Definition
x	Message vector $[x_0, \ldots, x_{N/2-1}]$
$x_{[i]}$	The i-th element of x
x	A ciphertext of x
X	A list of message vectors $\{x_0, \ldots, x_{n-1}\}$
$X_{[i]}$	The i-th message vector of X
X	A list of ciphertexts $\{x_0, x_1, \ldots, x_{n-1}\}$
$X_{[i]}$	The i-th ciphertext of X
$x * y$	$[x_0 \cdot y_0, \ldots, x_{N/2-1} \cdot y_{N/2-1}]$
$x + y$	$[x_0 + y_0, \ldots, x_{N/2-1} + y_{N/2-1}]$
$x - y$	$[x_0 - y_0, \ldots, x_{N/2-1} - y_{N/2-1}]$
$x \cdot y$	$[x_0 \cdot y_0 + \cdots + x_{N/2-1} \cdot y_{N/2-1}]$

$$S_a = \begin{bmatrix} x_{0,1} \\ x_{1,1} \\ \vdots \\ x_{m-1,1} \\ x_{0,2} \\ x_{1,2} \\ \vdots \\ x_{m-1,2} \\ \cdots \\ \cdots \\ \ddots \\ \cdots \\ x_{0,n_1} \\ x_{1,n_1} \\ \vdots \\ x_{m-1,n_1} \end{bmatrix}$$

$$S_b = \begin{bmatrix} x_{0,n_1+1} \\ x_{1,n_1+1} \\ \vdots \\ x_{m-1,n_1+1} \\ \cdots \\ \cdots \\ \ddots \\ \cdots \\ x_{0,n_1+n_2} \\ x_{1,n_1+n_2} \\ \vdots \\ x_{m-1,n_1+n_2} \\ y_0 \\ y_1 \\ \vdots \\ y_{m-1} \end{bmatrix}. \quad (1)$$

S_a and S_b consist of m samples of the form $\{x_{i,1}, x_{i,2}, \ldots, x_{i,n_1}\}$ and $\{x_{i,n_1+1}, \ldots, x_{i,n_1+n_2}, y_i\}$, respectively, where $i = 0, 1, \ldots, m-1$. Each column of S_a denote the features. The last column of S_b represents the label, and other columns of S_b represent the features. P_a cooperates with P_b to train a shared LR model without revealing the data privacy. Suppose $2(n_1 + n_2 + 1) \leq N$, the details of the proposed P^2 VCLR are described below.

Input: S_a and S_b for P_a and P_b respectively

Output: $[\xi_0^{(s)}, \xi_1^{(s)}, \ldots, \xi_{n_1}^{(s)}]$ and $[\xi_{n_1+1}^{(s)}, \xi_{n_1+2}^{(s)}, \ldots, \xi_{n_1+n_2}^{(s)}]$ for P_a and P_b respectively

Preprocessing:

1: P_a computes $l = 2^{\log(n_1+n_2+1)}$, $u = N/2l$, $v = m/u$, lets $\{x_i' = [1, x_{i,1}, x_{i,2}, \ldots, x_{i,n_1}, 0, 0, \ldots, 0] | \; i = 0, 1, \ldots, m-1\}$,

generates $\{sk_a, pk_a, rk_a, gk_a\} \leftarrow \mathrm{KeyGen}(N, Q)$, encrypts dataset S_a into v ciphertexts

$$\left\{ x_{a,i} = \mathrm{Enc}([x_{i\cdot u}', x_{i\cdot u+1}', \ldots, x_{(i+1)\cdot u-1}', \underbrace{\ }_{N/2}], pk_a) | \quad i = 0, 1, \ldots, v-2 \right\},$$

$x_{a,v-1} = \mathrm{Enc}([x_{(v-1)\cdot u}', x_{(v-1)\cdot u+1}', \ldots, x_m', \underbrace{0, 0, \ldots, 0}_{N/2}], pk_a)$,

lets

$\xi'^{(0)} = [\xi_0^{(0)}, \xi_1^{(0)}, \ldots, \xi_{n_1}^{(0)}, \underbrace{0, 0, \ldots, 0}_{l}]$,

encrypts the initial weight $\xi'^{(0)}$ into one ciphertext $\xi_a^{(0)} = \mathrm{Enc}([\xi'^{(0)}, \xi'^{(0)}, \ldots, \xi'^{(0)}], pk_a)$,

and sends N, Q, Δ, pk_a, rk_a, gk_a, s, $\{x_{a,i} | i = 0, 1, \ldots, v-1\}$, $\xi_a^{(0)}$ to P_b.

2: P_b computes $l = 2^{\log(n_1+n_2+1)}$, $u = N/2l$, $v = m/u$, lets

$$\left\{ x_i'' = [\underbrace{0, 0, \ldots, 0}_{n_1+1}, x_{i,n_1+1}, x_{i,n_1+2}, \ldots, x_{i,n_1+n_2}, \underbrace{0, 0, \ldots, 0}_{l}] \quad i = 0, 1, \ldots, m-1 \right\},$$

$$\left\{ y_i = [y_i, \underbrace{0, 0, \ldots, 0}_{l}] \quad i = 0, 1, \ldots, m-1 \right\},$$

sets data set S_b into $2v$ message vectors

$\{x_{b,i} = [x_{i\cdot u}'', x_{i\cdot u+1}'', \cdots, x_{(i+1)\cdot u-1}'', \underbrace{\ }_{N/2}]$ $i = 0, 1, \ldots, v-2\}$,

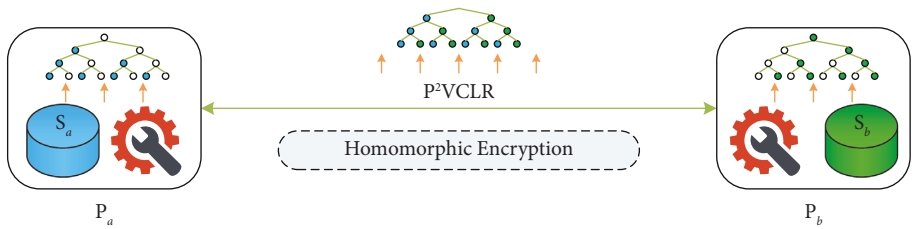

Figure 1: System architecture.

$x_{b,v-1} = [x''_{(v-1)\cdot u}, x''_{(v-1)\cdot u+1}, \ldots, x''_m, 0, 0, \ldots, 0]$,
$\{y_i = [y_{i\cdot u}, y_{i\cdot u+1}, \ldots, y_{(i+1)\cdot u-1}]_{N/2} \quad i = 0, 1, \ldots, v-2\}$,
$y_{v-1} = [y_{(v-1)\cdot u}, y_{(v-1)\cdot u+1}, \ldots, y_m, 0, 0, \ldots, 0]$,
lets
$\xi''^{(0)} = [0, 0, \ldots, 0_{n_1+1}, \xi^{(0)}_{n_1+1}, \xi^{(0)}_{n_1+2}, \ldots, \xi^{(0)}_{n_1+n_2}, 0, 0, \ldots, 0]_{N/2}$,
sets the initial weight $\xi''^{(0)}$ into one message vector
$\xi^{(0)}_b = [\xi''^{(0)}, \xi''^{(0)}, \ldots, \xi''^{(0)}]_{N/2}$,
sets the learning rate α into one message vector
$\alpha/m = [\alpha/m, \alpha/m, \ldots, \alpha/m_{n_1+n_2}, 0, 0, \ldots, 0]_{N/2}$,
lets
$$\left\{ w_i = [w_i, 0, 0, \ldots, 0]_l \quad i = 0, 1, 3, 5, 7 \right\},$$
sets the message vectors
$$\left\{ \omega_i = [w_i, w_i, \ldots, w_i]_{N/2} \quad i = 0, 1, 3, 5, 7 \right\},$$
sets the lists
$X_a = \{x_{a,0}, x_{a,1}, \ldots, x_{a,v-1}\}$,
$X_b = \{x_{b,0}, x_{b,1}, \ldots, x_{b,v-1}\}$,
$Y = \{y_0, y_1, \ldots, y_{v-1}\}$.

Training:

3: P_b computes $\xi^{(0)} = \text{Add\_Plain}(\xi^{(0)}_a, \xi^{(0)}_b)$
4: **for** $(i = 0$ to $v-1)$ **do**
5: P_b computes $X_{[i]} = \text{Add\_Plain}(X_{a,[i]}, X_{b,[i]})$
6: **end for**
7: **for** $(j = 0$ to $s-1)$ **do**
8: **for** $(i = 0$ to $v-1)$ **do**
9: P_b computes $D_{[i]} = \text{Mul}(\xi^{(j)}, X_{[i]}, rk_a)$
10: P_b computes $E_{[i]} = \text{Rot\_Sum\_1}(D_{[i]}, l, gk_a)$
11: P_b computes $F_{[i]} = \text{Approx\_Sigmoid}(E_{[i]}, \omega_0, \omega_1, \omega_3, \omega_5, \omega_7, rk_a)$
12: P_b computes $G_{[i]} = \text{Sub\_Plain}(F_{[i]}, Y_{[i]})$
13: P_b computes $H_{[i]} = \text{Rot\_Sum\_2}(G_{[i]}, l, gk_a)$
14: P_b computes $I_{[i]} = \text{Mul}(H_{[i]}, X_{[i]}, rk_a)$
15: **end for**
16: P_b computes $a = \text{Add\_Many}(I)$
17: P_b computes $b = \text{Rot\_Sum\_3}(a, l, gk_a)$
18: P_b computes $c = \text{Mul\_Plain}(b, \alpha/m, rk_a)$
19: P_b computes $\widehat{\xi}^{(j+1)} = \text{Sub}(\xi^{(j)}, c)$
20: P_b chooses random message vector $\delta^{(j+1)} = [\delta^{(j+1)}_0, \delta^{(j+1)}_1, \ldots, \delta^{(j+1)}_{N/2-1}]$
21: P_b computes $\varphi^{(j+1)} = \text{Sub\_Plain}(\widehat{\xi}^{(j+1)}, \delta^{(j+1)})$
22: P_b sends $\varphi^{(j+1)}$ to P_a
23: P_a computes $\varphi^{(j+1)} = \text{Dec}(\varphi^{(j+1)}, sk_a)$ to P_a
24: P_a sets $\widehat{\varphi}^{(j+1)} = [\varphi^{(j+1)}_{[0]}, \varphi^{(j+1)}_{[1]}, \ldots, \varphi^{(j+1)}_{[n_1+n_2]}, 0, 0, \ldots, 0]_l$
25: P_a sets $\widetilde{\varphi}^{(j+1)} = [\widehat{\varphi}^{(j+1)}, \widehat{\varphi}^{(j+1)}, \ldots, \widehat{\varphi}^{(j+1)}]_{N/2}$
26: P_a sets $\widetilde{\varphi}^{(j+1)} = \text{Enc}(\widetilde{\varphi}^{(j+1)}, pk_a)$
27: P_a sends $\widetilde{\varphi}^{(j+1)}$ to P_b
28: P_b sets $\widehat{\delta}^{(j+1)} = [\delta^{(j+1)}_{[0]}, \delta^{(j+1)}_{[1]}, \ldots, \delta^{(j+1)}_{[n_1+n_2]}, 0, 0, \ldots, 0]_l$
29: P_b sets $\widetilde{\delta}^{(j+1)} = [\widehat{\delta}^{(j+1)}, \widehat{\delta}^{(j+1)}, \ldots, \widehat{\delta}^{(j+1)}]_{N/2}$
30: P_b computes $\xi^{(j+1)} = \text{Add\_Plain}(\widetilde{\varphi}^{(j+1)}, \widetilde{\delta}^{(j+1)})$
31: **end for**

Reconstructing:

32: P_a sends $[\varphi^{(s)}_{[n_1+1]}, \varphi^{(s)}_{[n_1+2]}, \ldots, \varphi^{(s)}_{[n_1+n_2]}]$ to P_b
33: P_b computes $[\xi^{(s)}_{n_1+1}, \xi^{(s)}_{n_1+2}, \ldots, \xi^{(s)}_{n_1+n_2}] = [\varphi^{(s)}_{[n_1+1]}, \varphi^{(s)}_{[n_1+2]}, \ldots, \varphi^{(s)}_{[n_1+n_2]}] + [\delta^{(s)}_{[n_1+1]}, \delta^{(s)}_{[n_1+2]}, \ldots, \delta^{(s)}_{[n_1+n_2]}]$
34: P_b sends $[\delta^{(s)}_{[0]}, \delta^{(s)}_{[1]}, \ldots, \delta^{(s)}_{[n_1]}]$ to P_a
35: P_a computes $[\xi^{(s)}_0, \xi^{(s)}_1, \ldots, \xi^{(s)}_{n_1}] = [\varphi^{(s)}_{[0]}, \varphi^{(s)}_{[1]}, \ldots, \varphi^{(s)}_{[n_1]}] + [\delta^{(s)}_{[0]}, \delta^{(s)}_{[1]}, \ldots, \delta^{(s)}_{[n_1]}]$
36: **return**: $[\xi^{(s)}_0, \xi^{(s)}_1, \ldots, \xi^{(s)}_{n_1}]$ and $[\xi^{(s)}_{n_1+1}, \xi^{(s)}_{n_1+2}, \ldots, \xi^{(s)}_{n_1+n_2}]$ for P_a and P_b respectively

5. Performance Evaluation

We execute the performance comparisons among our P^2 VCLR scheme and existing schemes [9, 21]. We perform all experiments on a 64-bits Linux system machine with i7 CPU and 16 GB memory. For all experiments, we choose the initial weights $[\xi^{(0)}_0, \xi^{(0)}_1, \ldots, \xi^{(0)}_{n_1}] = [0, 0, \ldots, 0]$, $[\xi^{(s)}_{n_1+1}, \xi^{(s)}_{n_1+2}, \ldots, \xi^{(s)}_{n_1+n_2}] = [0, 0, \ldots, 0]$, the learning rate $\alpha = 0.15$, and the maximum number of iterations $s = 20$. The schemes [9, 21] choose the Paillier cryptosystem [25] to provide the additive HE operations, the proposed scheme

Table 2: Performance comparisons.

S_a	S_b	scheme	Training time	Accuracy	F1-score	AUC	No TTP
		[9]	1.27 min	74.1 %	85.1 %	0.57	×
Θ_1: $\{x_1 - x_4\}$	Θ_1: $\{x_5 - x_8, y\}$	[21]	2.18 min	74.1 %	85.1 %	0.56	√
		Ours	0.86 min	74.4 %	85.2 %	0.58	√
		[9]	2.20 min	91.3 %	77.5 %	0.96	×
Θ_2: $\{x_1 - x_5\}$	Θ_1: $\{x_6 - x_9, y\}$	[21]	3.41 min	90.9 %	75.3 %	0.96	√
		Ours	1.49 min	92.3 %	78.0 %	0.96	√
		[9]	11.13 min	82.7 %	60.1 %	0.88	×
Θ_3: $\{x_1 - x_8\}$	Θ_1: $\{x_9 - x_{15}, y\}$	[21]	21.32 min	82.7 %	60.1 %	0.89	√
		Ours	5.87 min	85.7 %	61.9 %	0.91	√

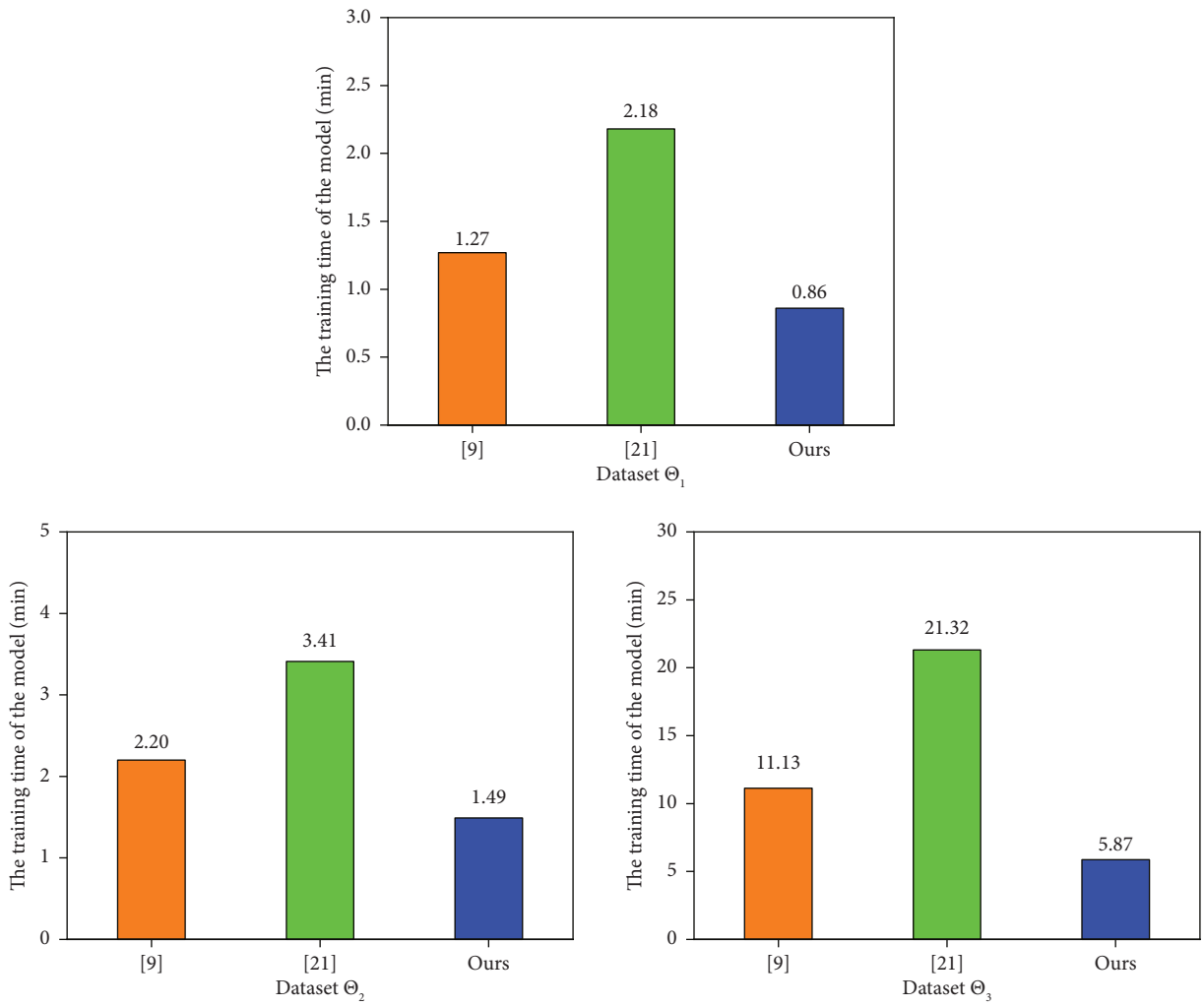

Figure 2: The training time of the model.

uses the Microsoft SEAL library [41] to instantiate the HE operations [29]. To achieve $\kappa = 80$ bits security, for the schemes [9, 21], we set the prime number $p, q = 512$ bits and $n = 1024$ bits; for the proposed scheme, we choose the polynomial-degree $N = 2^{15}$, the coefficient-modulus $Q = 520$, and the scaling factor $\Delta = 2^{40}$. On three publicly available datasets [30]: Θ_1 - Umaru Impact Study, Θ_2 - Myocardial Infarction from Edinburgh, and Θ_3 - Nhanes III, we compare the proposed scheme and schemes [9, 21] in terms of training time, accuracy, F1-score, AUC. P_a has the first 4 features $\{x_1 - x_4\}$ of all samples of Θ_1, P_b has the last 4 features and labels $\{x_5 - x_8, y\}$ of all samples of Θ_1; P_a has the first 5 features $\{x_1 - x_5\}$ of all samples of Θ_2, P_b has the last 4 features and labels $\{x_6 - x_9, y\}$ of all samples of Θ_2; P_a has the first 8 features $\{x_1 - x_8\}$ of all samples of Θ_3, P_b has the last 7 features and labels $\{x_9 - x_{15}, y\}$ of all samples of

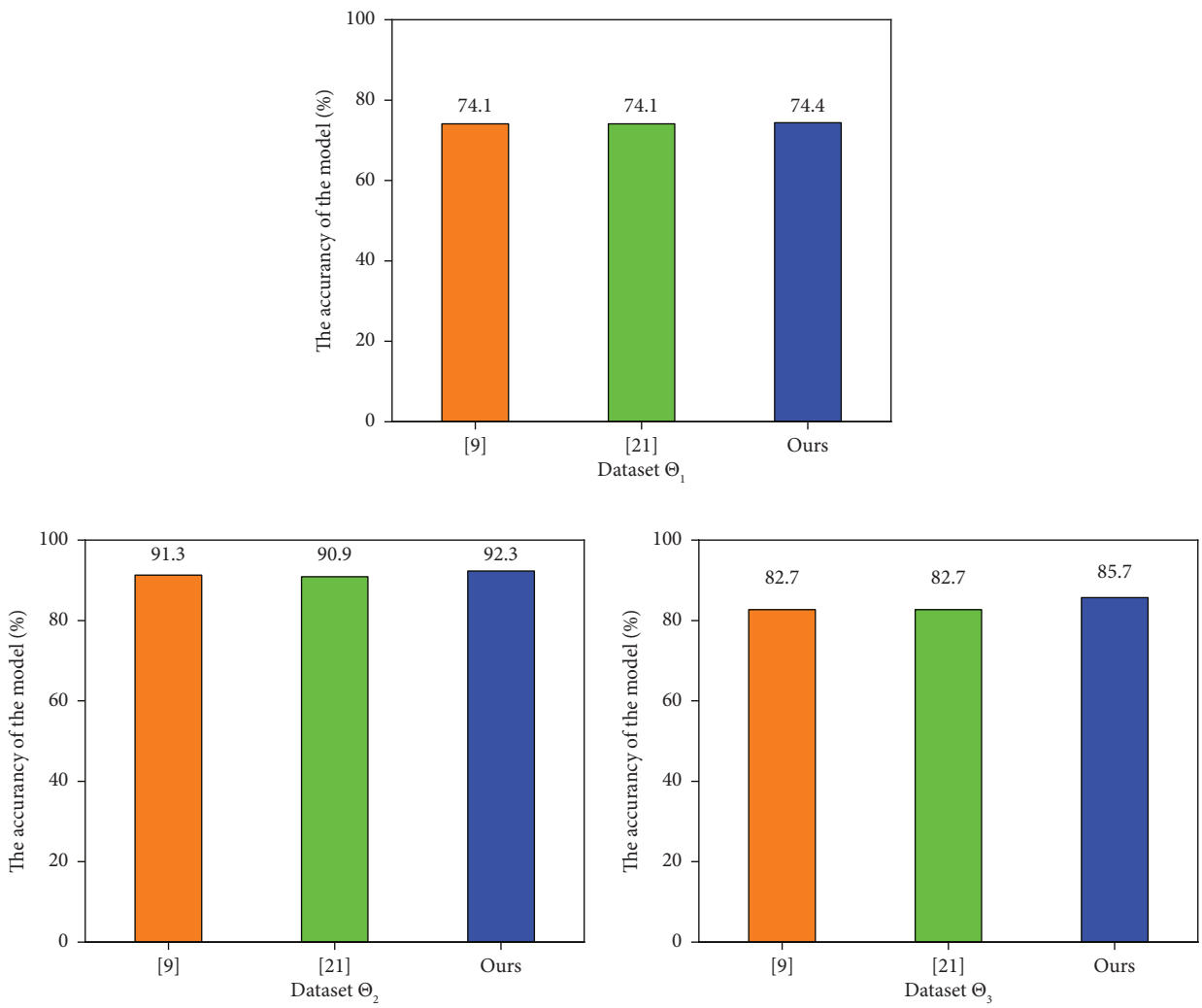

Figure 3: The accuracy of the model.

Θ_3. We get the validity of the experimental results by using 5-fold cross-validation. All experiment results are shown as the average of 10 experiments. The performance comparisons between the proposed scheme and schemes [9,21} are described in Table 2, in which " $\surd$" denotes "satisfied" and " $\times$" means "unsatisfied". From Table 2, we can see that our P^2 VCLR scheme outperforms existing schemes [9, 21] in both training time and model performance, and does not need a TTP coordinator.

From Figure 2, we can get that, for dataset Θ_1, in our scheme, the training time of the model is 0.86 min, which is decreased by nearly 32.3% and 60.6% compared with that of [9, 21], respectively; for dataset Θ_2, in our scheme, the training time of the model is 1.49 min, which is reduced by almost 32.3% and 56.3% in comparison to that of [9, 21], respectively; for dataset Θ_3, in our scheme, the training time of the model is 5.87 min, which is nearly 47.3% and 72.5% less than that of [9, 21], respectively.

From Figure 3, we can get that, for dataset Θ_1, in our scheme, the accuracy of the model is 74.4%, which has nearly 0.3% and 0.3% improvement compared with that of [9, 21], respectively; for dataset Θ_2, in our scheme, the accuracy of the model is 92.3%, which has an increase of almost 1.0% and 1.4% in comparison to that of [9, 21], respectively; for dataset Θ_3, in our scheme, the accuracy of the model is 85.7%, which is nearly 3.0% and 3.0% higher than that of [9, 21], respectively.

From Figure 4, we can get that, for dataset Θ_1, in our scheme, the F1-score of the model is 85.2%, which has nearly 0.1% and 0.1% improvement compared with that of [9, 21], respectively; for dataset Θ_2, in our scheme, the F1-score of the model is 78.0%, which has an increase of almost 0.5% and 2.7% in comparison to that of [9, 21], respectively; for dataset Θ_3, in our scheme, the F1-score of the model is 61.9%, which is nearly 1.8% and 1.8% higher than that of [9, 21], respectively.

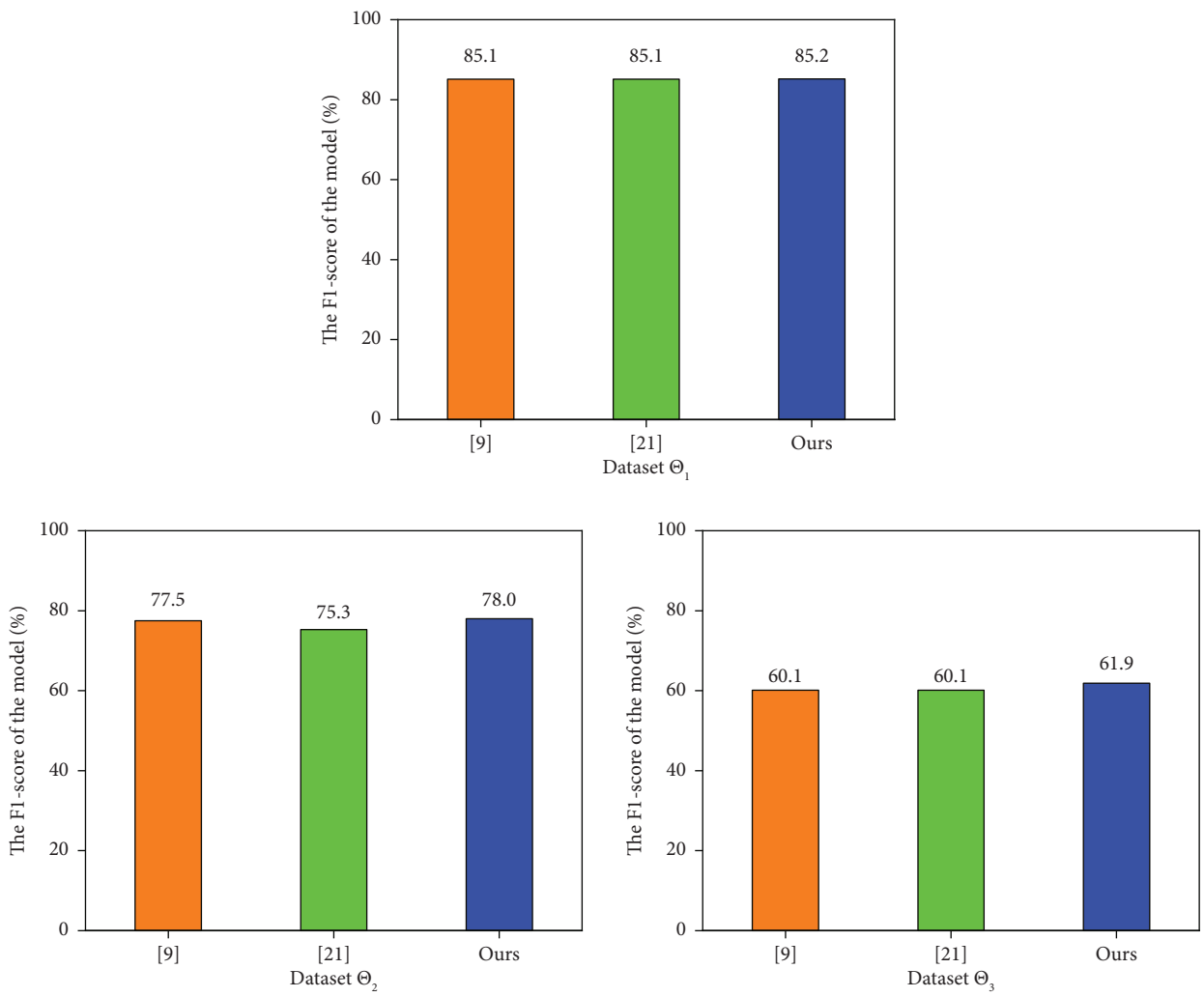

Figure 4: The F1-score of the model.

From Figure 5, we can get that, for dataset Θ_1, in our scheme, the AUC of the model is 0.58, which has nearly 0.01 and 0.02 improvement compared with that of [9, 21], respectively; for dataset Θ_2, in our scheme, the AUC of the model is 0.96, which is the same as that of [9, 21]; for dataset Θ_3, in our scheme, the AUC of the model is 0.91, which is nearly 0.03 and 0.02 higher than that of [9, 21], respectively.

6. Security Analysis

In the semi-honest model [42], we let the parties P_a and P_b know pk_a, rk_a, gk_a, and only P_a has sk_a. The proposed P^2 VCLR scheme belongs to secure two-party computation, which denotes an objective functionality $\mathcal{F} \cdot \{\mathcal{F}_a, \mathcal{F}_b\}$. For the inputs $\{x_a, x_b\}$, where x_a is from party P_a and x_b is from party P_b, the outputs $\{\mathcal{F}_a(x_a, x_b), \mathcal{F}_b(x_a, x_b)\}$ are random. $\mathcal{F}_a(x_a, x_b)$ is the output for P_a, and $\mathcal{F}_b(x_a, x_b)$ is for P_b, and neither party can know more private information than its output. According to the simulation-based security [43], we perform a security analysis of our P^2 VCLR scheme.

Definition 1. Let $\mathcal{F}$ be a deterministic functionality and Π be a secure two-party computation protocol to compute $\mathcal{F}$. Given P_a's input x_a, P_b's input x_b, and security level κ, the views of P_a and P_b in the protocol Π are denoted as $\mathcal{V}_a = \{\kappa, x_a, x_b\} = \{sk_a, pk_a, rk_a, gk_a, x_a, x_b, y_a\}$ and $\mathcal{V}_b = \{\kappa, x_a, x_b\} = \{pk_a, rk_a, gk_a, x_b, y_b\}$, where y_a and y_b are the messages received by P_a and P_b. We think that, in semi-honest model, Π can securely calculate $\mathcal{F}$ if there are the probabilistic polynomial-time (PPT) simulators $\mathcal{S}_a$ and $\mathcal{S}_b$, such that

$$\begin{aligned} \{\mathcal{S}_a(1^\kappa, x_a, \mathcal{F}_a(x_a, x_b))\}_{\kappa, x_a, x_b} &\cong \{\mathcal{V}_a(\kappa, x_a, x_b)\}_{\kappa, x_a, x_b} \\ \{\mathcal{S}_b(1^\kappa, x_b, \mathcal{F}_b(x_a, x_b))\}_{\kappa, x_a, x_b} &\cong \{\mathcal{V}_b(\kappa, x_a, x_b)\}_{\kappa, x_a, x_b}. \end{aligned} \tag{2}$$

Theorem 1. *Assuming that the P_a and P_b do not collude with each other, and the HE scheme (CKKS) [29] satisfies the semantic security, our P^2 VCLR scheme can ensure the security in semi-honest model.*

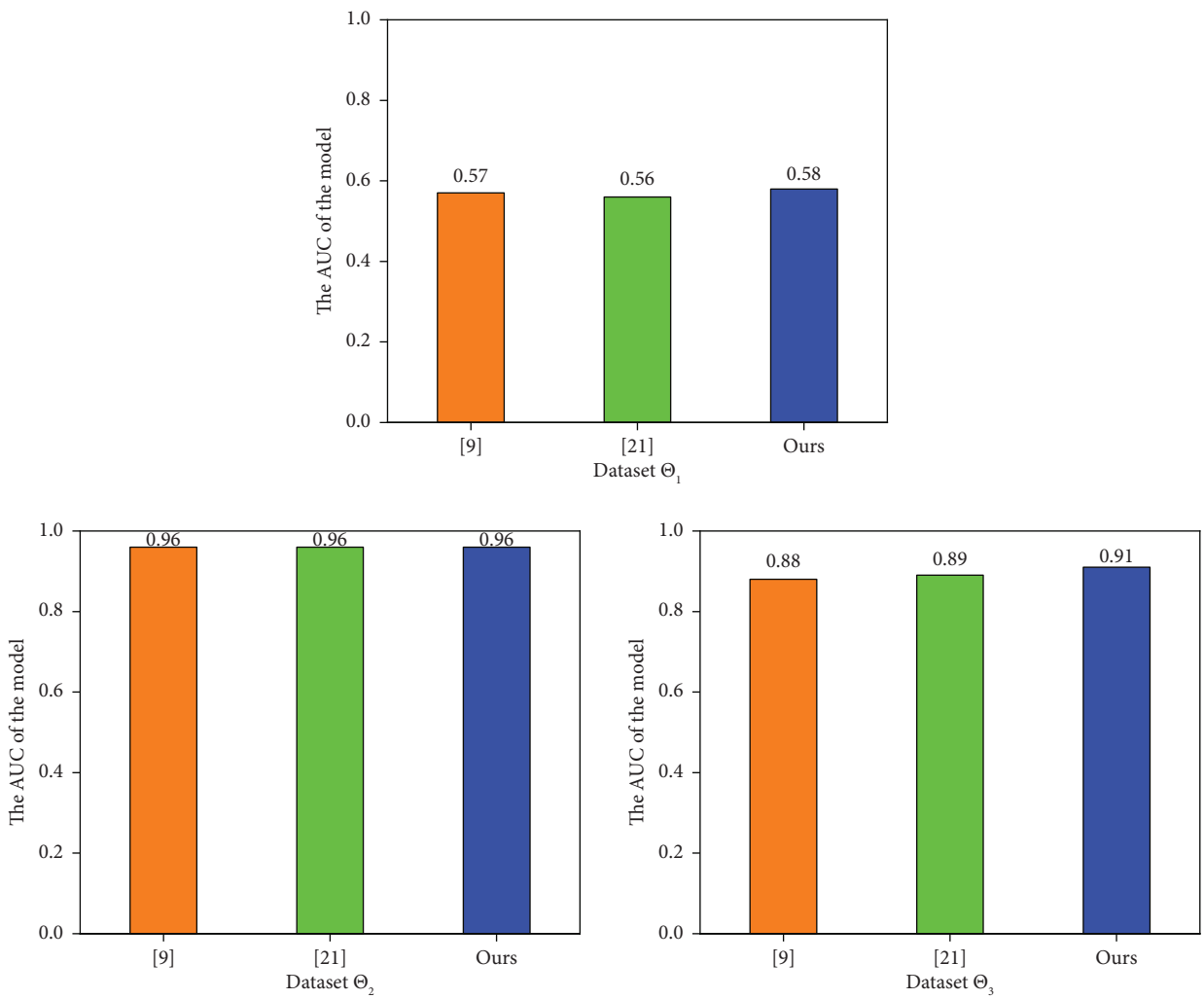

Figure 5: The AUC of the model.

Security Proof. Security proof of our P^2 VCLR scheme follows the simulation-based security [43]. We prove that we are able to build $\mathcal{S}_a$ and $\mathcal{S}_b$, such that

$$\begin{aligned}\left\{\mathcal{S}_{\mathcal{A}_a}(1^\kappa, y_a, sk_a)\right\}_{\kappa,z,sk_a} &\cong \left\{\mathcal{V}_{\mathcal{A}_a}(\kappa, z, sk_a)\right\}_{\kappa,z,sk_a}\\ \left\{\mathcal{S}_{\mathcal{A}_b}(1^\kappa, z, y_b)\right\}_{\kappa,z,sk_a} &\cong \left\{\mathcal{V}_{\mathcal{A}_b}(\kappa, z, sk_a)\right\}_{\kappa,z,sk_a},\end{aligned} \tag{3}$$

where $\mathcal{V}_{\mathcal{A}_a}$ and $\mathcal{V}_{\mathcal{A}_b}$ denote the views of $\mathcal{A}_a$ and $\mathcal{A}_b$, respectively. Next, we show that the above two equations are indistinguishable for the corrupted parties $\mathcal{A}_a$ and $\mathcal{A}_b$, respectively.

Against corrupted $\mathcal{A}_a$: We build $\mathcal{S}_a$ that, when given κ, $\mathcal{A}_a$'s input sk_a and $\mathcal{A}_a$'s output y_a, is able to simulate $\mathcal{A}_a$'s view in the execution of the protocol. In this respect, we then analyze $\mathcal{A}_a$'s view $\mathcal{V}_{\mathcal{A}_a}(\kappa, z, sk_a)$ in the execution of the protocol. The only message $\mathcal{A}_a$ gets is the ciphertext z. Therefore, $\mathcal{V}_{\mathcal{A}_a}(\kappa, z, sk_a)$ consists of $\mathcal{A}_a$'s secret key sk_a, random message vector r_a and ciphertext y_a. Given κ, sk_a, and y_a, $\mathcal{S}_{\mathcal{A}_a}$ generates a simulation of $\mathcal{V}_{\mathcal{A}_a}(\kappa, z, sk_a)$. $\mathcal{S}_{\mathcal{A}_a}$ encrypts $\mathcal{S}_{\mathcal{A}_a}$ with pk_a into y_a', and generates the output (sk_a, r_a, y_a'). Therefore, we can obtain two equations as follows:

$$\begin{aligned}\mathcal{V}_{\mathcal{A}_a}(\kappa, z, sk_a) &= (sk_a, r_a, y_a')\\ \mathcal{S}_{\mathcal{A}_a}(1^\kappa, y_a, sk_a) &= (sk_a, r_a, y_a').\end{aligned} \tag{4}$$

Through the above analysis, we are able to get that probability distribution of $\mathcal{A}_a$'s view and $\mathcal{S}_{\mathcal{A}_a}$'s output is indistinguishable. Therefore, the proposed P^2 VCLR scheme is secure against the corrupted $\mathcal{A}_a$ in semi-honest model.

Against corrupted $\mathcal{A}_b$: We build $\mathcal{S}_b$ that, when given κ, $\mathcal{A}_b$'s input z and $\mathcal{A}_b$'s output y_b, is able to simulate $\mathcal{A}_b$'s view in the execution of the protocol. For this reason, we analyze $\mathcal{A}_b$'s view $\mathcal{V}_{\mathcal{A}_b}(\kappa, z, sk_a)$ in the execution of the protocol. $\mathcal{A}_b$ does not receive any message vectors from $\mathcal{A}_a$. Therefore, $\mathcal{V}_{\mathcal{A}_b}(\kappa, z, sk_a)$ consists of $\mathcal{A}_b$'s input z and random message vector r_b. Given κ, z, and y_b, $\mathcal{S}_{\mathcal{A}_b}$ generates a simulation of $\mathcal{V}_{\mathcal{A}_b}(\kappa, z, sk_a)$ by outputting (z, r_b). Therefore, we have the following two equations:

$$\begin{aligned}\mathcal{V}_{\mathcal{A}_b}(\kappa, z, sk_a) &= (z, r_b)\\ \mathcal{S}_{\mathcal{A}_b}(1^\kappa, z, y_b) &= (z, r_b).\end{aligned} \tag{5}$$

Through the above analysis, we are able to get that probability distributions of $\mathcal{A}_b$'s view and $\mathcal{S}_{\mathcal{A}_b}$'s output are indistinguishable. Therefore, the proposed P^2 VCLR scheme is secure against the corrupted $\mathcal{A}_b$ in the semi-honest model.

7. Conclusion

In this paper, to improve the efficiency of the collaborative LR, based on an approximate HE algorithm, we propose a P^2 VCLR over vertically distributed data while realizing the security of training data and the privacy of model parameters for all parties. We then evaluate the proposed scheme on the public datasets. The evaluation results show that our P^2 VCLR scheme achieves a better performance in terms of joint training time and model performance in comparison to that of existing schemes [9, 21]. Specifically, the training time of the model is decreased by almost 32.3%-72.5%; the accuracy, F1-score, and AUC of the model have nearly 0.3% - 3.0%, 0.1% - 2.7% and 0 - 0.03 improvement, respectively. In the future, we will extend our method for supporting more complex ML, and deploy our scheme for practical applications.

Appendix

Input: $x, \omega_0, \omega_1, \omega_3, \omega_5, \omega_7, rk_i$

Output: $f(x)$

1: $x^2 = \mathrm{Mul}(x, x, rk_i)$

2: $x^4 = \mathrm{Mul}(x^2, x^2, rk_i)$

3: $x^6 = \mathrm{Mul}(x^2, x^4, rk_i)$

4: $\omega_7 x = \mathrm{Mul\_Plain}(x, \omega_7, rk_i)$

5: $\omega_7 x^7 = \mathrm{Mul}(\omega_7 x, x^6, rk_i)$

6: $\omega_5 x = \mathrm{Mul\_Plain}(x, \omega_5, rk_i)$

7: $\omega_5 x^5 = \mathrm{Mul}(\omega_5 x, x^4, rk_i)$

8: $\omega_3 x = \mathrm{Mul\_Plain}(x, \omega_3, rk_i)$

9: $\omega_3 x^3 = \mathrm{Mul}(\omega_3 x, x^2, rk_i)$

10: $\omega_1 x = \mathrm{Mul\_Plain}(x, \omega_1, rk_i)$

11: $\omega_0 + \omega_1 x = \mathrm{Add\_Plain}(\omega_1 x, \omega_0)$

12: $\omega_0 + \omega_1 x - \omega_3 x^3 = \mathrm{Sub}(\omega_0 + \omega_1 x, \omega_3 x^3)$

13: $\omega_0 + \omega_1 x - \omega_3 x^3 + \omega_5 x^5 = \mathrm{Add}(\omega_0 + \omega_1 x - \omega_3 x^3, \omega_5 x^5)$

14: $\omega_0 + \omega_1 x - \omega_3 x^3 + \omega_5 x^5 - \omega_7 x^7 = \mathrm{Sub}(\omega_0 + \omega_1 x - \omega_3 x^3 + \omega_5 x^5, \omega_7 x^7)$

15: return: $f(x) = \omega_0 + \omega_1 x - \omega_3 x^3 + \omega_5 x^5 - \omega_7 x^7$

Input: $x = [[[x_0, x_1, \ldots, x_{l-1}, x_l, x_{l+1}, \ldots, x_{2l-1}, \ldots, x_{(u-1)l}, x_{(u-1)l+1}, \ldots, x_{N/2-1}]]], l, gk_i$

Output: $y = [[[\sum_{i=}^{} 0^{l-1} x_i, \circ, \ldots, \circ\_l, \sum_{i=l}^{2l-1} x_i, \circ, \ldots, \circ, \ldots, \sum_{i=(u-1)l}^{N/2-1} x_i, \circ, \ldots, \circ]]]$

1: $y = x_{\bar{l}}$

2: **for** $(k = l/2;\ k \geq 1;\ k = k/2)$ **do**

3: $z = \mathrm{Rot\_Vector}(y, k, gk_i)$

4: $y = \mathrm{Add}(y, z)$

5: **end for**

6: **return**: y

Input:
$x = [[[x_0, 0, \ldots, 0, x_l, 0, \ldots, 0, \ldots, x_{(u-1)l}, 0, \ldots, 0]]], l, gk_i$

Output:
$y = [[[x_0, x_0, \ldots, x_0, x_l, x_l, \ldots, x_l, \ldots, x_{(u-1)l}, x_{(u-1)l}, \ldots, x_{(u-1)l\_l}]]]$

1: $y = x$

2: for $(k = l/2;\ k \geq 1;\ k = k/2)$ do

3: $z = \mathrm{Rot\_Vector}(y, -k, gk_i)$

4: $y = \mathrm{Add}(y, z)$

5: **end for**

6: **return**: y

Input:
$x = [[[x_0, x_1, \ldots, x_{l-1}, x_l, x_{l+1}, \ldots, x_{2l-1}, \ldots, x_{(u-1)l}, x_{(u-1)l+1}, \ldots, x_{N/2-1}]]], l, gk_i$

Output:
$y = [[[\sum_{i=0}^{u-1} x_{il}, \ldots, \sum_{i=0}^{u-1} x_{(i+1)l-1}, \ldots, \sum_{i=0}^{u-1} x_{il}, \ldots, \sum_{i=0}^{u-1} x_{(i+1)l-1\_l}]]]$

1: $y = x$

2: **for** $(k = N/2;\ k \geq l/2 + 1;\ k = k/2)$ **do**

3: $z = \mathrm{Rot\_Vector}(y, k, gk_i)$

4: $y = \mathrm{Add}(y, z)$

5: **end for**

6: **return**: y

Data Availability

Previously reported datasets were used to support this study and are available at https://doi.org/10.1186/s12920-018-0401-7. These prior studies (and datasets) are cited at relevant places within the text as references [30].

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work is supported by the National Key R\&D Program of China (Grant No. 2019YFE0113200) the National Natural Science Foundation of China (Grant No. U19B2021, No. 61901317), and the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2020A1515110496, No. 2020A1515110079).

References

[1] P. Mohassel and Y. Zhang, "SecureML: a system for scalable privacy-preserving machine learning," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 19–38, San Jose, CA, USA, May, 2017.

[2] J. M. Cort, A. Tchernykh, M. Babenko, B. Pulido-Gayt, and G. Radchenko, "Multi-cloud privacy-preserving logistic

regression," in *Proceedings of the 7th Russian Supercomputing Days*, pp. 457–471, Moscow, Russia, September, 2021.

[3] Y. Guan, "Application of logistic regression algorithm in the diagnosis of expression disorder in Parkinson's disease," in *Proceedings of the 2nd International Conference on Information Technology, Big Data and Artificial Intelligence*, pp. 1117–1120, Chongqing, China, December, 2021.

[4] E. Dumitrescu, S. Hué, C. Hurlin, and S. Tokpavi, "Machine learning for credit scoring: improving logistic regression with non-linear decision-tree effects," *European Journal of Operational Research*, vol. 297, no. 3, pp. 1178–1192, 2022.

[5] J. Feng, W. Zhang, Q. Pei, J. Wu, and X. Lin, "Heterogeneous computation and resource allocation for wireless powered federated edge learning systems," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3220–3233, 2022.

[6] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 1–2700, 2022.

[7] J. Du, F. R. Yu, X. Chu, J. Feng, and G. Lu, "Computation offloading and resource allocation in vehicular networks based on dual-side cost minimization," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1079–1092, 2019.

[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[9] S. Hardy, W. Henecka, H. Ivey-Law et al., "Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption," 2017, https://arxiv.org/abs/1711.10677.

[10] K. Yang, T. Fan, T. Chen, Y. Shi, and Q. Yang, "A quasi-Newton method based vertical federated learning framework for logistic regression," 2019, https://arxiv.org/abs/1912.00513.

[11] K. Mandal and G. Gong, "PrivFL: practical privacy-preserving federated regressions on high-dimensional data over mobile networks," in *Proceedings of the 10th ACM SIGSAC Conference on Cloud Computing Security Workshop*, pp. 57–68, London, England, November 2019.

[12] Y. Zhang, G. Bai, X. Li, C. Curtis, and R. K. L. Ko, "PrivColl: practical privacy-preserving collaborative machine learning," in *Proceedings of the 25th European Symposium on Research in Computer Security*, pp. 399–418, Guildford, UK, September 2020.

[13] Y. Liu, T. Fan, T. Chen, Q. Xu, and Q. Yang, "FATE: an industrial grade platform for collaborative learning with data protection," *Journal of Machine Learning Research*, vol. 22, no. 226, pp. 1–6, 2021.

[14] M. D. Cock, R. Dowsley, A. C. A. Nascimento, D. Railsback, J. W. Shen, and A. Todoki, "High performance logistic regression for privacy-preserving genome analysis," *BMC Medical Genomics*, vol. 14, no. 1, pp. 1–18, 2021.

[15] C. Wang, J. Xu, and L. Yin, "A secure cloud-edge collaborative logistic regression model," in *Proceedings of the IEEE Congress on Cybermatics/14th IEEE International Conference on Internet of Things/14th IEEE International Conference on Cyber, Physical and Social Computing/17th IEEE International Conference on Green Computing and Communications/7th IEEE International Conference on Smart Data*, pp. 244–253, Electric Network, Melbourne, Australia, December, 2021.

[16] R. Zhu, C. Jiang, X. Wang, S. Wang, H. Zheng, and H. Tang, "Privacy-preserving construction of generalized linear mixed model for biomedical computation," *Bioinformatics*, vol. 36pp. 128–135, supplement_1, 2020.

[17] S. Yang, B. Ren, X. Zhou, and L. Liu, "Parallel distributed logistic regression for vertical federated learning without third-party coordinator," 2019, https://arxiv.org/abs/1911.09824.

[18] C. Chen, B. Wu, L. Wang, C. Chen, and B. Zhang, "Nebula: a scalable privacy-preserving machine learning system in ant financial," in *Proceedings of the 29th ACM International Conference on Information and Knowledge Management, Electr Network*, pp. 3369–3372, Ireland, October, 2020.

[19] Q. Li, Z. Huang, W. J. Lu et al., "HomoPAI: a secure collaborative machine learning platform based on homomorphic encryption," in *Proceedings of the 36th International Conference on Data Engineering*, pp. 1713–1717, Dallas, USA, April, 2020.

[20] Q. J. Wei, Q. Li, Z. P. Zhou, Z. Q. Ge, and Y. G. Zhang, "Privacy-preserving two-parties logistic regression on vertically partitioned data using asynchronous gradient sharing," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1379–1387, 2020.

[21] C. Chen, J. Zhou, L. Wang et al., "When homomorphic encryption marries secret sharing: secure large-scale sparse logistic regression and applications in risk control," in *Proceedings of the 27th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 2652–2662, Singapore, August, 2021.

[22] A. R. Ghavamipour, F. Turkmen, and X. Jiang, "Privacy-preserving logistic regression with secret sharing," *BMC Medical Informatics and Decision Making*, vol. 22, no. 1, pp. 89–11, 2022.

[23] D. He, R. Du, S. Zhu, M. Zhang, K. Liang, and S. Chan, "Secure logistic regression for vertical federated learning," *IEEE Internet Computing*, vol. 26, no. 2, pp. 61–68, 2022.

[24] H. Sun, Z. Wang, Y. Huang, and J. Ye, "Privacy-preserving vertical federated logistic regression without trusted third-party coordinator," in *Proceedings of the 6th International Conference on Machine Learning and Soft Computing*, pp. 132–138, Singapore, January, 2022.

[25] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the Advances in Cryptology - EUROCRYPT 1999: International Conference on the Theory and Application of Cryptographic techniques*, pp. 223–238, Prague, Czech Republic, May, 1999.

[26] A. C. Yao, "Protocols for secure computations," in *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pp. 1–5, Chicago, Illinois, USA, November, 1982.

[27] Z. Li, Z. Huang, C. Chen, and C. Hong, "Quantification of the leakage in federated learning," 2019, https://arxiv.org/abs/1910.05467.

[28] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[29] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2017: 23rd International Conference on the Theory and Application of Cryptology and Information Security*, pp. 409–437, Hong Kong, China, December, 2017.

[30] A. Kim, Y. Song, M. Kim, K. Lee, and J. H. Cheon, "Logistic regression model training based on the approximate homomorphic encryption," *BMC Medical Genomics*, vol. 11, no. S4, pp. 83–31, 2018.

[31] M. Joye and B. Libert, "Efficient cryptosystems from 2k-th power residue symbols," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 76–92, Athens, Greece, May, 2013.

[32] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1175–1191, Dallas, Texas, USA, November, 2017.

[33] B. Dan, S. Laur, and J. Willemson, "Sharemind: a framework for fast privacy-preserving computations," in *Proceedings of the 13th European Symposium on Research in Computer Security*, pp. 192–206, Málaga, Spain, October, 2008.

[34] M. De Cock, R. Dowsley, C. Horst et al., "Efficient and private scoring of decision trees, support vector machines and logistic regression models based on pre-computation," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 217–230, 2019.

[35] D. Reich, A. Todoki, R. Dowsley, M. D. Cock, and A. Nascimento, "Privacy-preserving classification of personal text messages with secure multi-party computation: an application to hate-speech detection," in *Proceedings of the 33rd International Conference on Neural Information Processing Systems*, pp. 3757–3769, Vancouver, Canada, December, 2008.

[36] H. Chen, W. Dai, M. Kim, and Y. Song, "Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 395–412, London, United Kingdom, November, 2019.

[37] W. Fang, C. Chen, J. Tan et al., "A hybrid-domain framework for secure gradient tree boosting," 2020, https://arxiv.org/abs/2005.08479.

[38] E. Boyle, N. Gilboa, and Y. Ishai, "Function secret sharing," in *Proceedings of the Advances in Cryptology – EUROCRYPT: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 337–367, Sofia, Bulgaria, April, 2015.

[39] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, pp. 265–284, Springer, New York, NY, USA, 2006.

[40] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 1–23, French Riviera, June, 2010.

[41] Microsoft Research and W. A. Redmond, "Microsoft SEAL (release 4.0)," mar, 2022, https://github.com/Microsoft/SEAL.

[42] O. Goldreich, *Foundations of Cryptography: Volume.I, Basic Applications*, Cambridge University Press, Cambridge , UK, 2006.

[43] A. Datta, J. C. Mitchell, and A. Ramanathan, "On the relationships between notions of simulation-based security," *Journal of Cryptology*, vol. 21, pp. 492–546, 2008.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4542705, 13 pages
https://doi.org/10.1155/2022/4542705

Research Article

Compression Domain Reversible Robust Watermarking Based on Multilayer Embedding

Qianwen Li,[1] **Xiang Wang**,[2] **and Qingqi Pei**[1]

[1]*School of Telecommunications Engineering, Xidian University, Xi'an 710071, China*
[2]*School of Cyber Engineering, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Xiang Wang; wangxiang@xidian.edu.cn

Received 23 May 2022; Revised 22 June 2022; Accepted 25 July 2022; Published 28 August 2022

Academic Editor: He Li

The integration of data sensing, communication, and computing (SCC) is a requirement for the IoT to provide a high quality of service. However, there are still data security issues in SCC integration, where data are vulnerable to leakage during sensing, communication, and computing, and the leaked data are difficult to be copyrighted and traced to the source of leakage. In this study, we consider the copyright protection problem in multimedia data transmission and propose a robust reversible watermarking algorithm based on multilayer embedding in the compression domain. In the first stage, the robust watermark is embedded into the mid-frequency coefficients, and then, the auxiliary information to revert the robust embedding is embedded into the high-frequency coefficients. To improve robustness and reduce embedding distortion, we propose a coefficient selection method, by which the watermark and the recovery information are embedded in different DCT-quantized coefficients according to the texture complexity. Experiment results indicate that the proposed method performs better than some state-of-the-art RRW methods.

1. Introduction

As one of the strategic emerging industries with important global development, the Internet of Things (IoT) technology is rapidly penetrating into various application areas, from people's daily lives to national strategic industries, and in many ways, also driving the world's development progress. IoT uses communication technologies such as local networks or the Internet to connect sensors [1–3], controllers, machines [4, 5], people, and objects together in new ways, forming a network where people are connected to things and things are connected to things. The integration of data sensing, communication, and computing (SCC) is a requirement for the IoT to provide a high quality of service. However, there are still security issues in SCC integration [6–10], such as node location leakage in data sensing, data leakage in data communication, and authentication. These privacy and security issues have an impact on the development of IoT. Digital watermarking, as a lightweight algorithm, can effectively solve the problems such as data authentication after data leakage. Existing watermarking algorithms can be classified into the robust watermarking algorithm, reversible watermarking algorithm, and robust reversible watermarking algorithm according to the characteristics of watermarking.

Robust watermarking algorithms require high robustness, which means it is possible to extract the correct watermarks when the marked image is attacked [11]. Robust watermarking schemes based on spatial domain mainly utilize some statistical characteristics of the images (e.g., focus or centroid of the image). Because the spatial domain is more intuitive and simple, most of the studies focus on it. However, the transform domain is more robust to compression and quantify attacks. Thus, the transform domain-based method achieved more attention [12, 13].

However, the robust watermark always introduces irreversible distortions to the cover images, which cannot be tolerated in some special applications, such as medical image system, law enforcement, and military image. Reversible watermarking [14] is proposed to overcome this issue, by

which the cover image could be recovered after watermark extraction. There are many relative researches have been proposed so far, mainly including four categories: compression based [15–17], integer transform based [18–21], histogram shifting (HS) based [14, 22–24], and prediction-error expansion (PEE) [25]. Compression-based technology exploits the embedded space by lossless compression of a specific area of the cover image, and then, this area is replaced by the compressed image and the watermark. This kind of method cannot efficiently use the redundant information of the image itself, so its embedding efficiency is low. Different expansion algorithm is one of the representative schemes of integer transform-based researches. This algorithm groups pixels into pairs and the watermarks are embedded into the expansion error of pixel pairs. Later works involve changing pixel pairs into pixel blocks to increase capacity. The histogram translation algorithm embeds watermarking information by changing the histogram formed by an attribute of the host image. This attribute may be only the value of pixels, or it may be the prediction error of the image. Prediction-error expansion (PEE) is one of the representative works. The histogram is constructed by counting the prediction errors of the pixels, and then, a part of the area in the histogram is shifted to create space for embedding the watermark. The method is characterized by large embedded capacity and low complexity of the algorithm. However, all these methods are so fragile that the watermarking cannot be extracted after being attacked.

For solving the poor robustness of reversible watermarking, a new technique named robust reversible watermarking (RRW) is proposed. By RRW, the cover images can be recovered if the marked images do not suffer from attacks, and the robust watermarks are robust against some normal attacks such as image compression, geometric attacks, and unavoidable addition of random noise. As a result, at the decoder side, both the watermarks extraction and image recovery can be achieved in the case of no attacks.

To our knowledge, the RRW methods mainly include two categories: generalized histogram shifting (GHS) and multilayer watermarking (MLW). GHS achieves good robustness by increasing the shifting distance of partial bins in the statistical quantity histogram, by which extra space for tolerance is created around the embedded position. When the image is distorted, the watermark is supposed to be extracted correctly as long as the distortion of the histogram does not exceed the fault-tolerant area. One of the representative results of such methods is histogram rotation (HR) [26] proposed by Bender et al., which is based on the patchwork theory [27] and modulo-256 addition. Their scheme can achieve reversibility and robustness by using a circular interpretation of bijective transformations. However, to avoid the overflow/underflow problems, the so-called salt-and-pepper noise occurs. Later on, Ni et al. [28] improved Zeng et al.'s scheme by utilizing different bit-embedding strategies for groups of pixels with different pixel grayscale value distributions together with error correction codes. Experimental results show this method had good robustness in the absence of salt-and-pepper noise. The other is redundant histogram shifting (RHS) [29], which is based on the traditional histogram shifting and gets more redundancy by expanding the distance of shifting. Experiment results show a good performance of robustness. For this method can be extended to the transform domain to improve robustness, some RRW schemes have been developed based on this framework [30, 31]. However, these methods require a lot of additional information (e.g., location maps) to be transmitted over additional secure channels. Therefore, no longer suitable for many applications.

As for MLW, Coltuc proposed the relevant framework in reference [13], which contains two embedding stages: the robust embedding stage and the reversible embedding stage. As shown in Figure 1, the first is the robust watermarking stage, where we embed the watermark information W by the robust watermarking algorithm. Then, the reversible watermarking algorithm is used to embed additional information RI to recover the original image. Finally, the watermarked image is generated. In the case of no attacks, the robust watermark can be extracted from the marked image, and the decoder exactly recovers the cover image. In the case of attacks, the reversibility is lost, but the robust watermark is also supposed to be extracted. One of the advantages of this framework is that the existing excellent robust and reversible watermarking methods could be directly introduced because of the two independent stages. However, Coltuc et al.'s method has its own shortcomings. The reversible watermark in stage 2 directly consists of the distortion from the first stage. Because the watermark information is too large, a reversible watermark (RW) scheme with a large capacity is required, but this will cause a considerable distortion. In addition, the robust and the reversible watermarking use the same embedding domains; thus, the two stages are not independent and interfere with each other.

As shown above, there are a large number of RRW methods, but few algorithms are proposed specifically for JPEG image. In this study, we propose a new reversible robust watermarking scheme for JPEG images. The reversible watermarks and robust watermarks are embedded into the coefficients of different frequency bands, respectively. Meanwhile, the algorithm preferentially selects the region with complex image texture for robust watermark embedding and the smooth texture region for reversible watermark embedding. That will cause less distortion. Moreover, a new robust watermarking is proposed in the study, which needs less information to invert both the robust and reversible watermarking in the second stage.

The rest of this study is organized as follows: in Section 2, the framework of MLW is introduced in detail. In Section 3, the proposed scheme is presented in detail. Experiment results compared with Zeng et al.'s RRW method are given in Section 4. Finally, conclusions are drawn.

2. Preliminaries

The MLW algorithm [12] proposed by Coltuc et al. is briefly introduced in this section. The framework of MLW includes two embedding stages: reversible embedding stage and robust embedding stage.

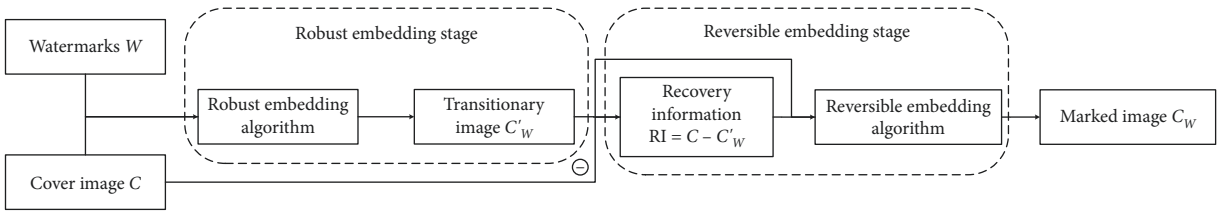

Figure 1: The framework of Coltuc et al.'s RRW method.

As shown in Figure 1, a watermark W is embedded into the cover image C by a robust watermarking method to generate a transitionary image C_W', and then, the recovery information $R_I = C - C_W'$ is hidden in the image C_W' by the reversible watermarking method. In the decoder, as Figure 2 shows, the recovery information R_I can be extracted from C_W as well as recovering the transitionary image C_W'. Then, the original image C can be recovered according to $C = C_W' + R_I$.

2.1. Embedding Procedure

2.1.1. Robust Embedding. The cover image is divided to 8×8 blocks and the DCT coefficients of each block are computed. One bit of watermark can be embedded into two coefficients from the middle-band frequencies of one block. For instance, a bit of "1" is embedded if the difference of these two coefficients is positive and "0" otherwise. Specifically, for two coefficients c_1 and c_2 of a 8×8 block, one bit of watermark w is embedded as follows:

$$(c_1', c_2') = \begin{cases} (c_1, c_2), & \text{if } c_1 - c_2 > 0 \text{ and } w = 1, \\ (c_2, c_1), & \text{if } c_1 - c_2 \le 0 \text{ and } w = 1, \\ (c_1, c_2), & \text{if } c_1 - c_2 \le 0 \text{ and } w = 0, \\ (c_2, c_1), & \text{if } c_1 - c_2 > 0 \text{ and } w = 0, \end{cases} \tag{1}$$

where c_1' and c_2' denote the marked coefficients. Figure 3 shows two examples of the embedding process, and the two framed coefficients are the selected coefficients c_1 and c_2. In the case of $c_1 > c_2$, when embedding bit 0, the positions of two coefficients are swapped; otherwise, the positions remain unchanged. In the case of $c_1 \le c_2$, when embedding bit 0, the positions of two coefficients remain unchanged; otherwise, they are swapped.

2.2. Reversible Embedding. As shown in Figure 1, in this stage, the recovery information $R_I = C - C_W'$, which is the difference between C and C_W', is first generated. Then, R_I is losslessly compressed to get the reversible watermark R. The RRW relies on the reversible watermarking stage's embedding capacity; thus, a reversible watermarking algorithm with high capacity is demanded. Specifically, C_W' is partitioned into pairs of pixels, and each pair (c_1', c_2') is transformed as follows:

$$\begin{cases} c_1'' = (m+1)c_1' - mc_2', \\ c_2'' = (m+1)c_2' - mc_1', \end{cases} \tag{2}$$

where $m > 1$ is a fixed integer to control EC.

The watermark $r \in [-m, m]$ is embedded as follows:

$$(c_{w1}, c_{w2}) \longrightarrow (c_1'' + r, c_2''), \tag{3}$$

and after all bits of the compressed information R are embedded, the marked image is generated.

2.3. Extracting Procedure. In the case of the marked image C_W suffers no distortion, as shown in Figure 2, the reversible extracting procedure is first implemented. The same as the embedding procedure in stage 2, the marked image C_W is partitioned into pairs of pixels, and for each pixel pair, the compressed information R is extracted as follows:

$$r = ((m+1)c_{w1} + mc_{w2}) mod (2m+1), \tag{4}$$

and the extracted watermark R is then decompressed to get the recovery information R_I, and the transitionary image C_W' is recovered as follows:

$$\begin{cases} c_1' = \lfloor \dfrac{(m+1)c_{w1} + mc_{w2}}{2m+1} \rfloor, \\ c_2' = \lfloor \dfrac{(m+1)c_{w2} + mc_{w1}}{2m+1} \rfloor, \end{cases} \tag{5}$$

where $\lfloor * \rfloor$ is the floor operation.

After reversible decoding, the watermark W could be extracted from the transitionary image C_W' by a robust extracting process. Specifically, C_W' is divided into 8×8 blocks and the DCT coefficients of each block are computed. For each block, the watermarking bit is extracted according to the difference between the two selected coefficients. If this difference is positive, the embedded information is "1," and otherwise, the embedded information is "0." Finally, the original image is recovered as $C = R_I + C_W'$.

In the case of marked image C_W with distortion, the original image C and the transitionary image C_W' could not be restored, but the watermark W can be extracted from the distorted image directly, as shown in Figure 4.

3. Proposed Method

As aforementioned, Coltuc et al.'s algorithm has its own shortcomings. First, the two embedding stages shared the same embedding domain, which leads to additional distortion. At decoder side actually will face two kinds of noises: the attacks from outside and the interference of the reversible embedding. Second, the spatial domain embedding process is not suitable to be directly introduced to JPEG images.

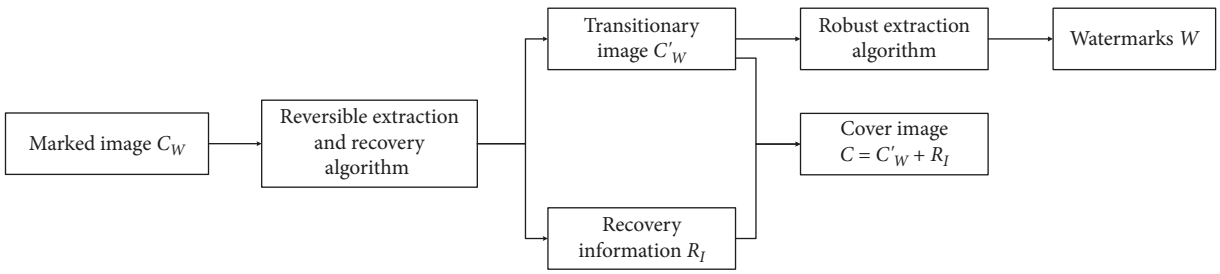

Figure 2: Decoder without distortion.

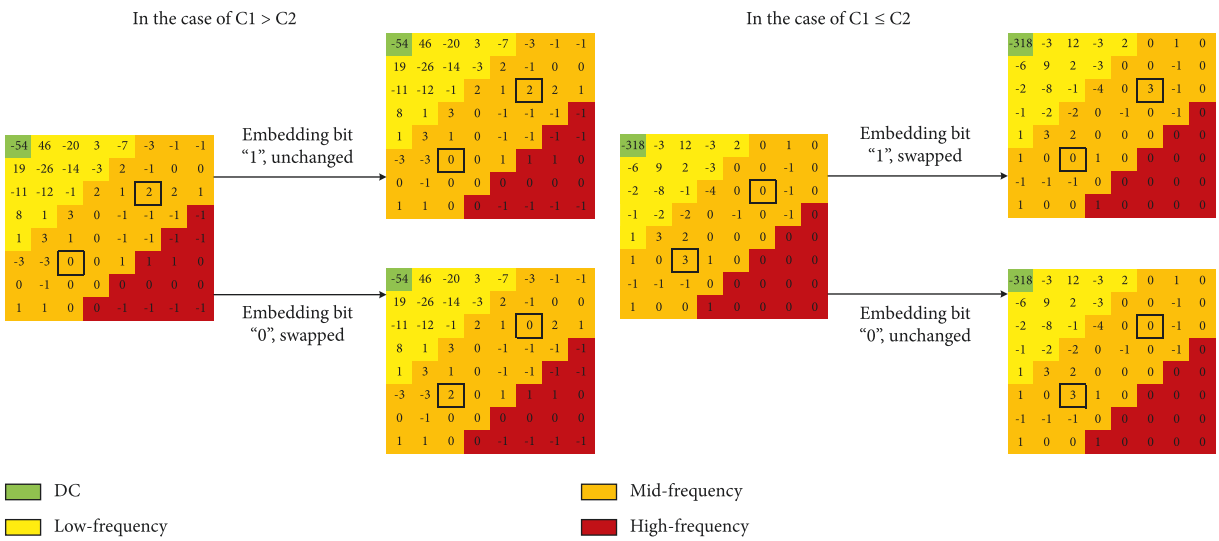

Figure 3: Robust embedding.

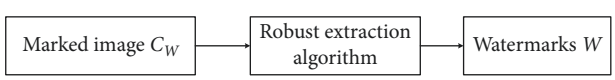

Figure 4: Decoder with distortion.

To this end, a RRW scheme for JPEG images is presented in this section. This scheme focuses on the compressed domain and embeds watermarks in the DCT-quantized coefficients. The proposed method follows the Coltuc et al.'s MLW framework and overcomes some shortcomings.

As Figure 5 shows, in the JPEG compression process, the source image is divided into 8×8 sized nonoverlapping blocks, for the pixels in each block, the DCT will be performed. Then, the DCT coefficients are quantified by using a quantization table, which is the cause of the image loss. After the entropy coding, the JPEG image is formed. The proposed method is applied to the quantized coefficients, and these coefficients are divided into two independent embedding domains, one for robust embedding and the other for reversible embedding.

3.1. Embedding Procedure. The embedding procedure roughly contains three steps: coefficients preprocessing, robust embedding, and reversible embedding. This section will introduce them one by one.

3.2. Stage 1 (Coefficients Selection). The DCT-quantized coefficients of the block B_i are zigzag arranged to generate a vector C_i. As shown in Figure 6, the vector could easily be divide into four regions: the low frequency C_i^l marked in yellow, the medium frequency for robust embedding C_i^{ro} marked in orange, the medium frequency for reversible embedding C_i^{re} marked in red, and the high frequency C_i^h marked in bronzing. The energy is concentrated in the low frequency coefficients C_i^l, which always refers to the part with large scale information (e.g., the background region). Thus, data embedding into low-frequency coefficients can generate visible artifacts. Coefficients in this part will stay unchanged. For the high-frequency region C_i^h, which always represents the small-scale detail information of the images, such as noise, edge, and jump part). The coefficients in this part will also remain unchanged because changing them affects the efficiency of entropy coding. Moreover, we use C_i^h to predict the texture complexity of each block as follows:

$$B_i \in \begin{cases} B^s, & if\ g \leq G; \\ B^c, & if\ g > G; \end{cases} \tag{6}$$

where we set $G > 0$ as the threshold to distinguish smooth block B^s and complex block B^c, and $g = \sum_{c_k \in C^h} |c_k|$. is used to predict the texture complexity of each block. Obviously, the larger g is, the more complex block texture, which indicates

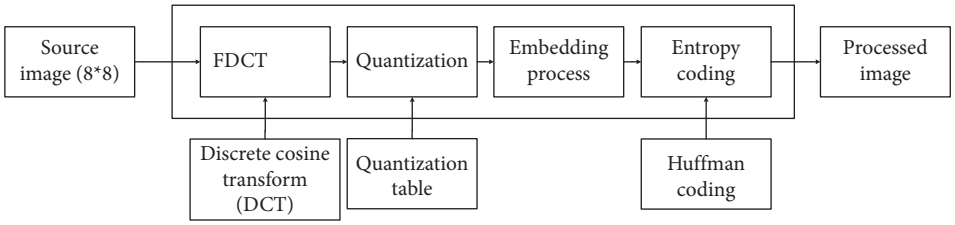

Figure 5: The position of our embedding process throughout the JPEG compress procedure.

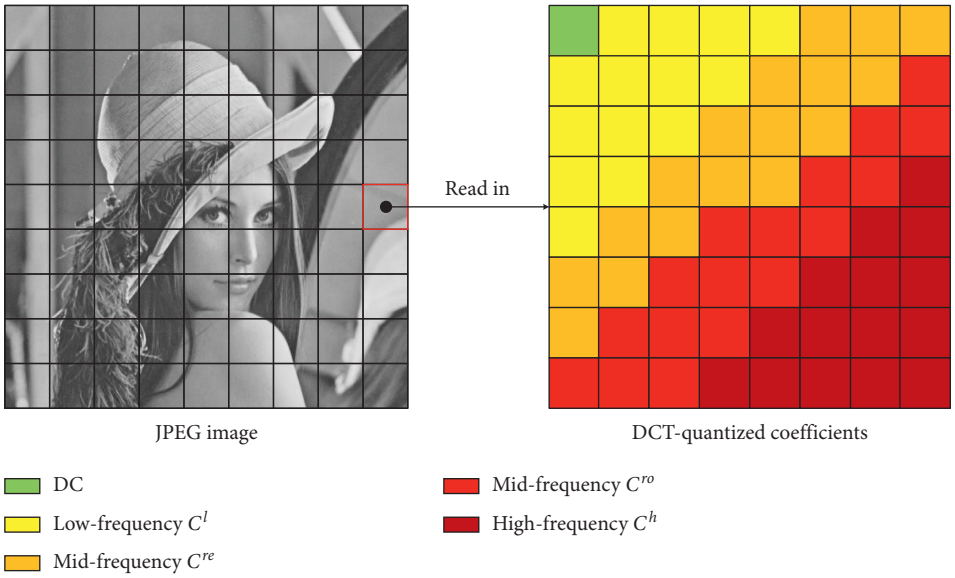

Figure 6: Frequency segmentation in a block.

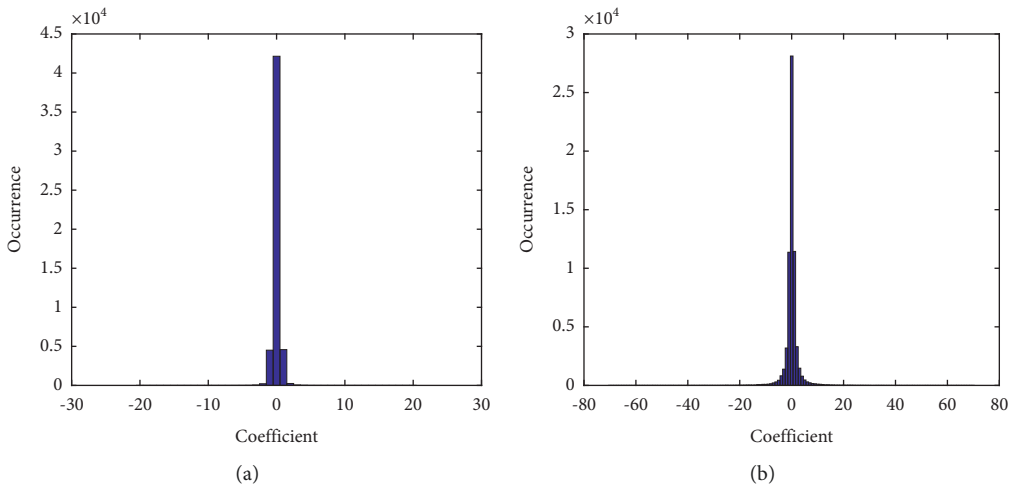

Figure 7: Coefficients histogram of region C^{re} (a) and region C^{ro} (b) for Lena.

the richer block information.The medium frequency coefficients in C^{ro} are robust against many attacks, which are selected to carry the robust watermarks. In addition, because the area with higher textural information usually has higher just noticeable difference (JND), we only use C^{ro} of the blocks from set B^c for robust embedding to ensure the high visual image quality. The reversible watermark in this scheme is embedded by the classical histogram shift (HS). For HS methods, the histogram with higher peak value and small variance produces higher performance. Thus, we use the coefficients of region C^{re} in smooth block B^s to embed reversible watermark, because the high-frequency coefficient in smooth area has a small variance. Figure 7 shows the comparison between the histogram of C^{re} and C^{ro}.

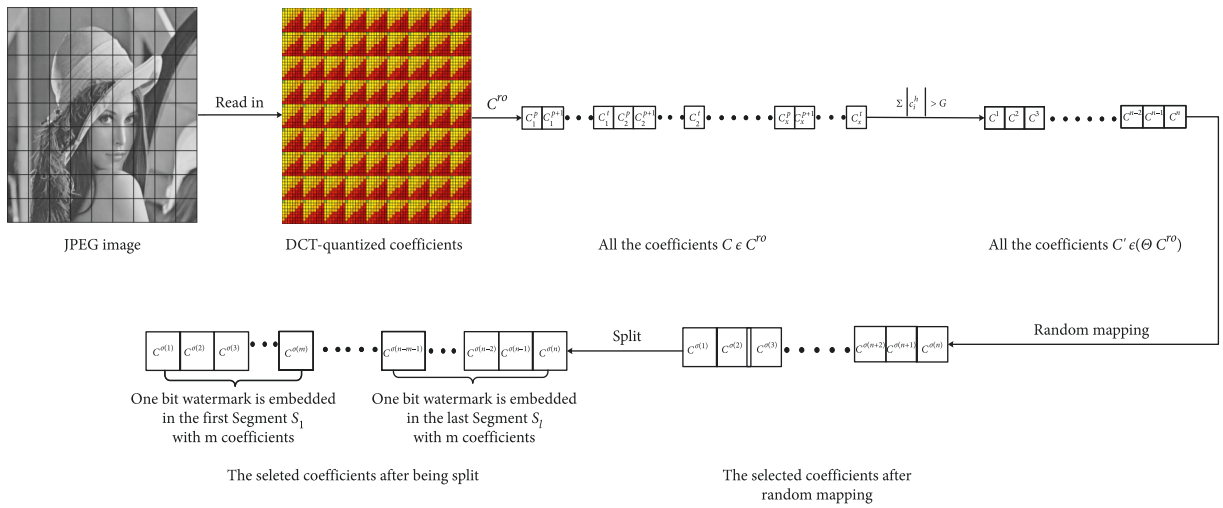

Figure 8: The diagram of robust embedding.

Therefore, the coefficients of medium frequency region C^{re} marked in red in Figure 6 from smooth block B^s are used for reversible embedding.

3.3. Stage 2 (Robust Embedding). The block B_i includes two independent embedding part: a robust embedding part $C_i^{ro} = \{c_i^p, c_i^{p+1}, \ldots, c_i^t\}$. and a reversible embedding part $C_i^{re} = \{c_i^{t+1}, c_i^{t+2}, \ldots, c_i^q\}$., where p, q, and t represent the position of the coefficient in the vector C_i. The robust watermark is embedding into C^{ro} of the complex blocks. We use the set Ω to denote these coefficients: $C_i^{ro} \in \Omega, if\ B_i \in B^c$. Suppose there are n coefficients in Ω. We use a random mapping as follows: $\{1, 2, \ldots, n\} \Rightarrow \{\sigma(1), \ldots, \sigma(2), \sigma(n)\}$, and the coefficients are arranged as a random long vector $\{c^{\sigma(1)}, c^{\sigma(2)}, \ldots, c^{\sigma(n)}\}$.. Then, to improve the robustness, we partition the coefficients into l segments S_k with m coefficients according to the robust watermarks length l, where $m = \lfloor n/l \rfloor$, $k \in \{0, \ldots, l-1\}$, and $\{c^{k\times m+1}, c^{k\times m+2}, \ldots, c^{(k+1)\times m}\} \in S_k$. Details are shown in Figure 8. Each coefficients c^i in the kth segment S_k is modified to embed the kth bit watermark $w_k \in [0, 1]$ as follows:

$$c_w^i = \begin{cases} c^i + \delta_k, & \text{if } w_k = 1 \text{ and } c^i \in S_k, \\ c^i - \delta_k, & \text{if } w_k = 0 \text{ and } c^i \in S_k. \end{cases} \tag{7}$$

δ_k is the modification value of each segment, which is calculated by the threshold T as follows:

$$\delta_k = \lfloor \frac{T - \left|\sum c^i\right|}{m} \rfloor, \tag{8}$$

where $\sum = \sum_{i=k\times m+1}^{(k+1)\times m} (k \in \{0, \ldots, l-1\})$. For the reversibility, δ_k in each segment must be recorded. After embedding, the sum of coefficients in each segment is greater than or equal to a threshold T.

It is worth noting that the coefficients will stay unchanged if the sum of the original coefficients of a segment exceeds or equals to the threshold requirement, i.e., the modification $\delta = 0$. After the watermark embedding is completed, the related inverse operation is performed on the coefficients in each segment to restore the position of the coefficients in each block. Afterwards, the robust embedding procedure is completed.

3.4. Stage 3 (Reversible Embedding). In reversible embedding stage, auxiliary information L, which is the information to erase the robust embedding distortion at the decoder side, is as reversible watermark. With the help of the auxiliary information L, the extraction of the watermarks w and recovery of the original image could be achieved. The auxiliary information L consists of δ_i when each bit of robust watermark is embedded:

$$L = \{\delta_1, \delta_2, \cdots, \delta_l\}. \tag{9}$$

The auxiliary information L is losslessly compressed as the reversible watermarks and transformed into a 0–1 sequence $\beta = (\beta_1, \ldots, \beta_l)$ with length l. Then, the reversible watermarks β are embedded in all the coefficients in the C^{re} of smooth block $B_i \in B^s$ by the classical HS-based reversible watermarking method. The set $\Phi = \{C_i^{re}, \text{if } B_i \text{in } B^s\}$. More specifically, the reversible embedding process is performed as follows:

$$c_w^{i'} = \begin{cases} c^i + \beta_j \times (T1 + 1), & \text{if } c^i \in \Phi \text{ and } c^i \in (0, T1], \\ c^i - \beta_j \times (T1 + 1), & \text{if } c^i \in \Phi \text{ and } c^i \in [-T1, 0), \\ c^i + (T1 + 1), & \text{if } c^i \in \Phi \text{ and } c^i > T1, \\ c^i - (T1 + 1), & \text{if } c^i \in \Phi \text{ and } c^i < T1, \end{cases} \tag{10}$$

where $\beta_j \in [0, 1]\,(j = (1, \ldots, l))$ is the reversible watermark, and $T1$ is the threshold controlling the EC (embedding capacity) of HS method.

Noticed that, in consideration of the entropy coding in JPEG compress procedure, the more zero coefficients are, the smaller size of the JPEG image is. Thus, we skip the

situation when $c^i = 0$, which will control the size of the watermarked image. As for the problem of overflow/underflow that most watermarking schemes must face, our algorithm does not need to worry about it because it works in the transform domain of the JPEG image.

After the above operations, all the watermarks are embedded in the coefficients. The last step is to reintegrate the DCT coefficients and rewrite them into the JPEG image.

3.5. Extracting Procedure. As for the decoding side, there are two kinds of cases that should be mentioned. In the case of no attacks, it contains the watermark extraction and image recovery. After preprocessing the DCT-quantized coefficients as mentioned in Section 3.1, the reversible watermarks should firstly be extracted:

$$\beta = \begin{cases} 0, & \text{if } c_w^{i'} \in [-T1, T1] \text{ and } c_w^{i'} \neq 0, \\ 1, & \text{if } c_w^{i'} \in (-2 \times T1 - 1, -T1) \text{ or } c_w^{i'} \in (T1, 2 \times T1 + 1). \end{cases} \tag{11}$$

The auxiliary information L is obtained after the decompression of the reversible watermarks. Meanwhile, the coefficient $c^i \in \Phi$ is recovered by the following equation:

$$c^i = \begin{cases} c_w^{i'} - (T1 + 1), & \text{if } c_w^{i'} \in (T1, +\infty), \\ c_w^{i'} + (T1 + 1), & \text{if } c_w^{i'} \in (-\infty, -T1). \end{cases} \tag{12}$$

According to Section 3.1, the robust watermark is extracted only by the following equation:

$$w = \begin{cases} 0, & \text{if } \sum c_w^i < 0, \\ 1, & \text{if } \sum c_w^i \geq 0. \end{cases} \tag{13}$$

Finally, with help of the auxiliary information L, the coefficient $c_{\sigma(i)}^{ro}$ is recovered by the following equation:

$$c^i = \begin{cases} c_w^i - \delta_k, & \text{if } w = 1, \\ c_w^i + \delta_k, & \text{if } w = 0, \end{cases} \tag{14}$$

where the definition of δ_k is as shown in equation (9). With the related inverse operation, the coefficients can be back to their original positions and the coefficients $c^i \in \Omega$ can be restored.

In the case of the marked image is distorted, the original image could not be recovered. However, the watermark is expected to be extracted according to equation (14) owning to the robustness of statistical property.

3.6. Procedures of Embedding and Extraction. The embedding procedure is described as follows:

Step 1. The JPEG image I is read in and each JPEG compression unit is treated as a processing block B_i.

Step 2. Zigzagly arranging each block to generate a vector C_i. Each vector is divided into 4 regions $(C^l, C^{ro}, C^{re}, C^h)$ as mentioned before. Then, using the coefficients in region C^h to predict the texture complexity of each block as equation (6).

Step 3. Picking out all the coefficients in the region C^{ro} of complex blocks, then integrating them into a long vector. After random mapping, the vector is then split into separated segments.

Step 4. As shown in equation (8), the robust watermarks w will be embedded in each separated segment in turn. As $w = 1$, the coefficients in the segment are modified so that its sum is greater than the threshold T; otherwise, it is less than the threshold $-T$.

Step 5. Noticed that the following auxiliary information should be recorded as reversible watermark: the value of the modification of each segment δ_k.

Step 6. The reversible watermark will be embedded in the region C^{re} of smooth blocks $B_i \in \Phi$ by the traditional HS method as shown in equation (11).

Step 7. After robust embedding and reversible embedding, reintegrate the DCT coefficients and rewrite them into the JPEG image. The watermarked image is obtained.

The extraction scheme is the inverse of the embedding scheme as follows:

Step 1. Referring to steps 1, 2, and 3 in embedding procedure, the regions C^{ro} and C^{re} are obtained.

Step 2. The reversible watermark should be extracted first. Using the traditional HS extraction and recovery method, auxiliary information can be obtained and coefficients in the region C^{re} of smooth blocks can be restored.

Step 3. Referring to step 4 in the embedding procedure, the robust watermark can be extracted by judging the sign of the sum of the coefficients in the segment, as shown in equation (13).

Step 4. According to auxiliary information, coefficients in the region C^{ro} of complex blocks are recovered by the related inverse operation.

Step 5. Finally, reintegrate the DCT coefficients and rewrite them into the JPEG image. The watermarked is obtained and the original image is restored.

It is worth mentioning that the original image may not be recovered if the watermarked image is attacked. However, the watermark is also supposed to be extracted.

4. Experimental Results and Discussion

This section presents experimental results for the proposed scheme. The proposed method is evaluated with embedding capacity from 200 bits to 1000 bits with an interval of 100 bits. Notice that, Coltuc et al.'s method does not perform well in JPEG images, which is explained earlier. Thus, the performance of the proposed scheme will be compared with Zeng et al.'s RHS method implemented in the compressed domain. For Zeng et al.'s method, the block size is fixed to 8×8 in consideration of JPEG procedure, and only the

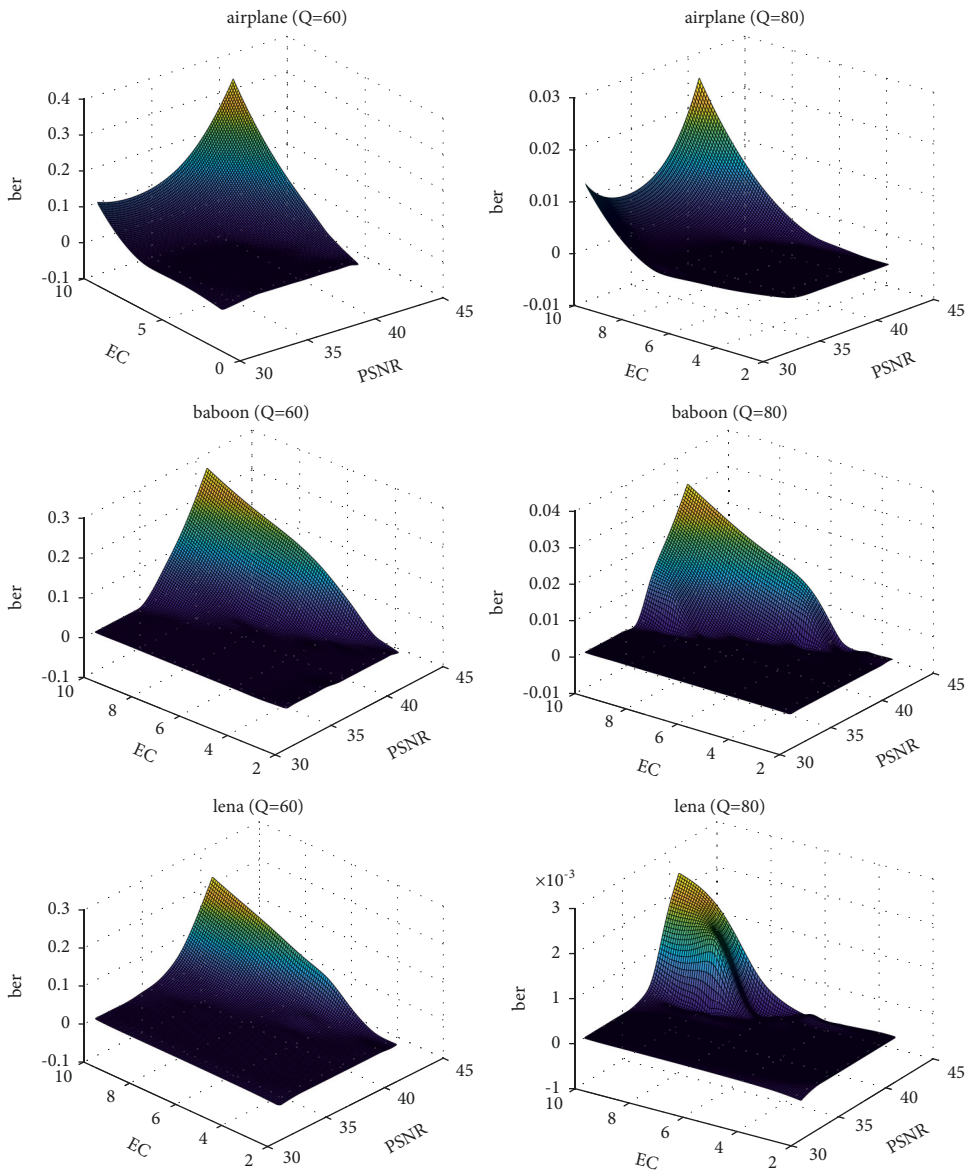

Figure 9: Trend of BER with the changes of the EC and PSNR.

coefficients in the region C^{ro} are used for the sake of fair comparison. We implement the method by Matlab and three 512×512 sized JPEG images (lena, baboon, and airplane) serve as test images, which are compressed with a quality factor of 95%. We change the embedding intensities to obtain different BERs and PSNRs both for the proposed method and Zeng et al.'s method. We change the variables G and T to control the PSNR of the proposed method. The threshold $T1$, which controls the EC in reversible embedding stage, is set as a fixed number ($T1 = 1$), because it has little effect on the image.

4.1. Robustness against JPEG Recompression. The proposed scheme is first evaluated the robustness against JPEG recompression. The bit error rate (BER) is adopted to estimate the robustness:

$$ber = \frac{l_e}{l_w}, \tag{15}$$

where l_e and l_w are the number of error bits and watermark bits, respectively. The trend of BER with the changes of the EC and PSNR for different images is shown in Figure 9. As mentioned before, to generate different PSNRs, the variables controlling the embedding intensity are varied within a certain range. Specifically, T is varying from 30 to 130 and the scope of G is based on the complexity of the image. As the axis of the EC is fixed, the BER increases with the growth of PSNR. It is because the embedding intensity decreases with the PSNR increasing, resulting in lower robustness. Furthermore, as the axis of the PSNR is fixed, the BER increases with the growth of EC. This is because the robustness of the algorithm decreases as the embedding

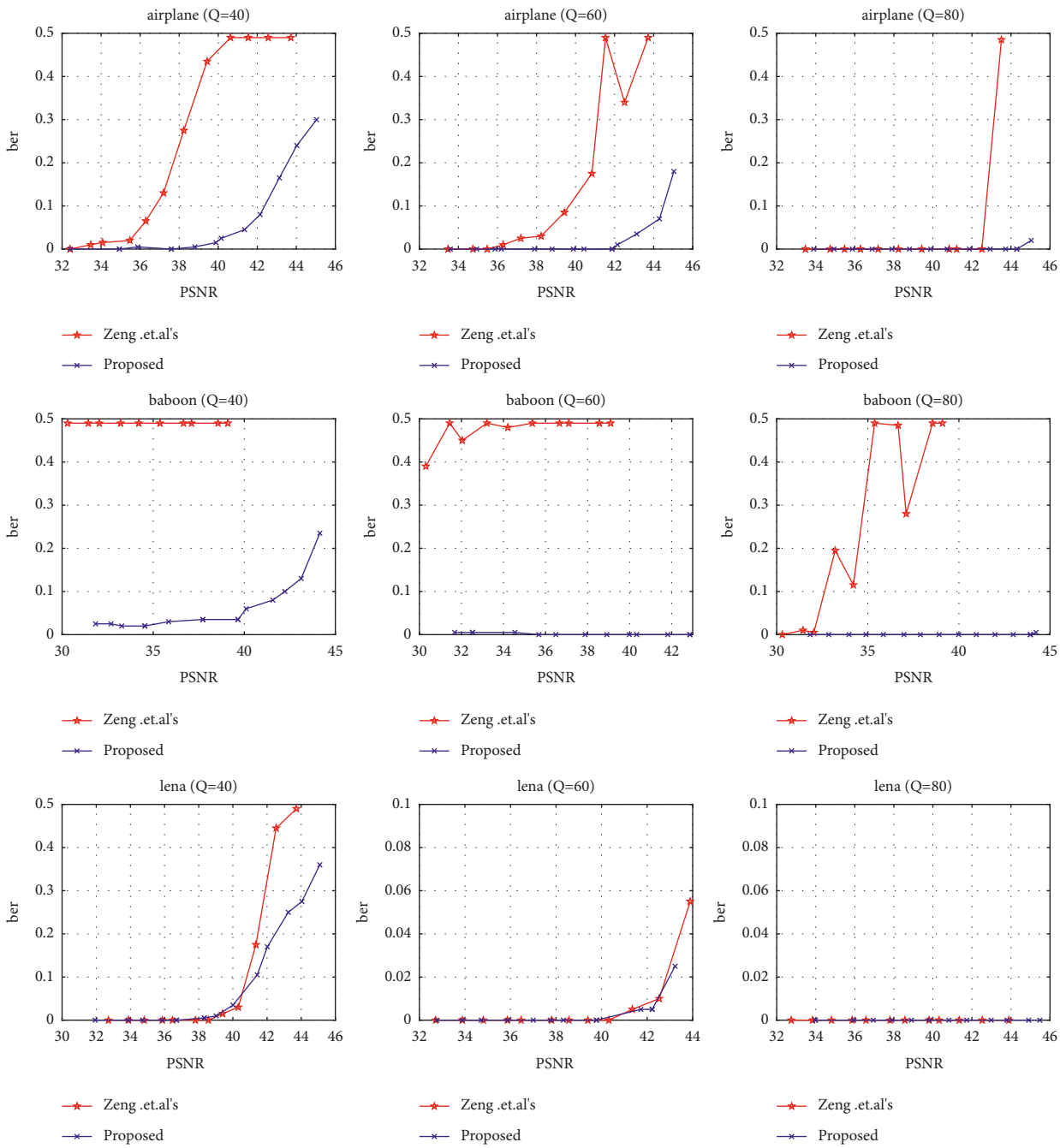

Figure 10: Comparison under different PSNRs at EC is 200 bits.

capacity EC increases when the PSNR is fixed, which leads to an increase in BER.

Figure 10 shows the comparison performance with BER vs. Figure 11PSNR at the EC of 200 bits and 500 bits. The proposed method outperforms the Zeng et al.'s method as the PSNR increases for the test images in most situations, especially for the textural image (baboon). In the case of the 80% JPEG compression, the proposed method has no error bits for 200 and 500 bits. As for the compression is to 60%, the correctness still can arrive at 100% only controlling the PSNR below 40 for the EC of 200 bits, and the corresponding PSNR might be lower when the EC is 500 bits. Even at 40% JPEG compressing, the proposed method also could keep the error rate low when the PSNR is below 36 for the EC of 200 bits. For Zeng et al.'s method, the BER quickly increases to around 50% when the PSNR arrives at a critical point, which means all the bits are wrong. The performance of Zeng et al.'s embedding scheme depends on the distribution of the histogram determined by the variance. The smaller the variance values, the better the performance of the data hiding scheme. Therefore, the performance for textural images is not satisfactory when using Zeng et al.'s method.

Referring to Figure 12, the comparisons at different JPEG Figure 13quality factors are presented. In this

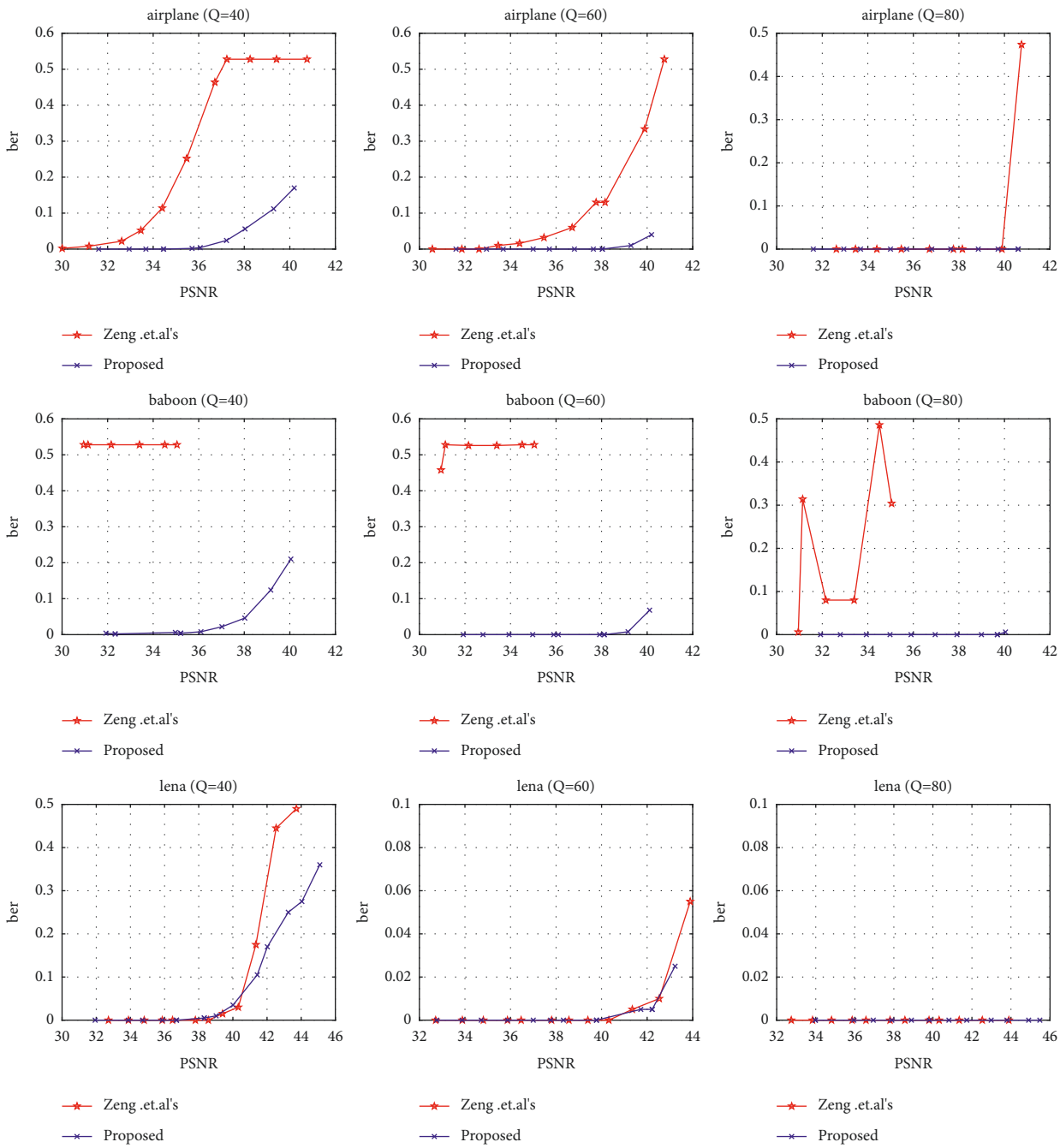

Figure 11: Comparison under different PSNRs at EC is 500 bits.

comparison, the PSNR is set to around 34 dB. It is obvious that the proposed method performs much better. For Zeng et al.'s method, the correct rate dropped quickly with the quality factor decrease, especially for the textural image baboon. This can be explained by comparing the threshold at decoding side: T and G for Zeng et al.'s method and 0 for the proposed method. Table 1 lists partial sum of the coefficients and partial arithmetic average difference of the coefficients with EC of 200 bits for image Lena when the PSNR is around 34. Here, S_o, S_w, and S_c represent the sum of the coefficients before embedding, after embedding and after JPEG compression with the 80% quality factor, and A_o, A_w, and A_c respectively represent the arithmetic average difference of the coefficients. We can see that even at 80% JPEG compression, S_c and A_c reduce quickly, which means the threshold at decoding side must be well designed for Zeng et al.'s method. Table 2 lists BER in different thresholds in the 80% quality factor compression with EC of 200 bits for image Lena, and the PSNR is also set to around 34. It could be found that for Zeng et al.'s method, the high accuracy could

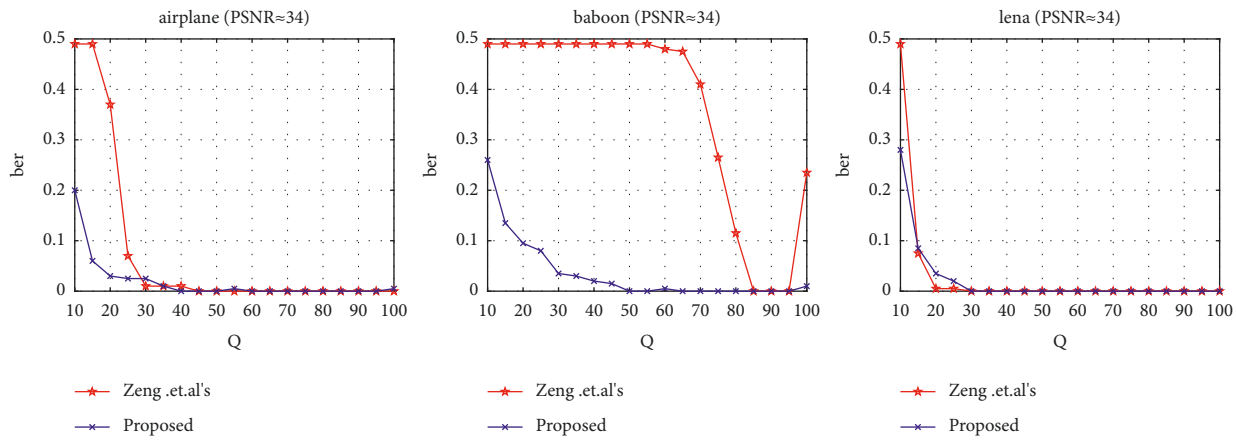

Figure 12: Comparison under different quality factors at EC is 200 bits.

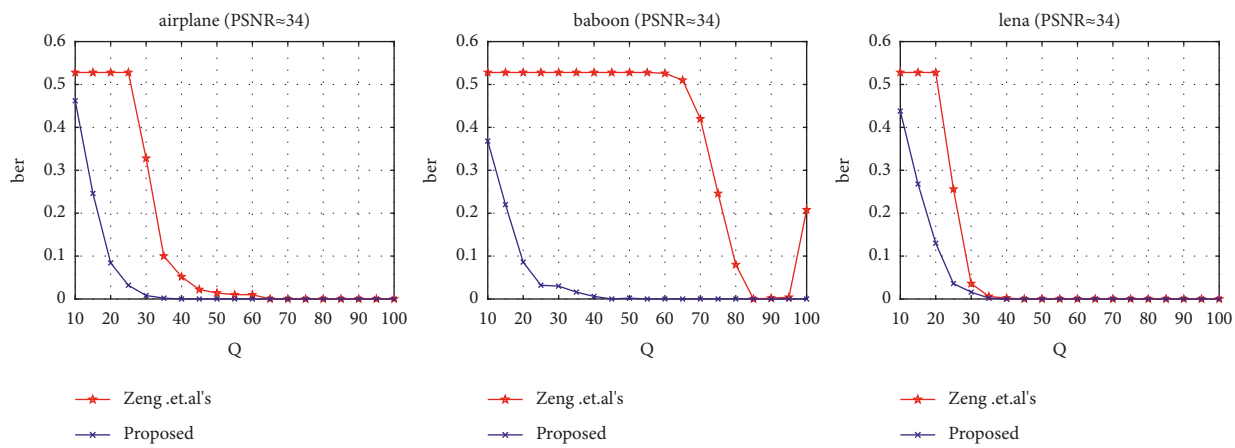

Figure 13: Comparison under different quality factors at EC is 500 bits.

Table 1: Sum of the coefficients and arithmetic average difference of the coefficients in the 80% quality factor compression.

EC = 200 bits						EC = 500 bits					
The proposed method			RHS			The proposed method			RHS		
S_o	S_w	S_c	A_o	A_w	A_c	S_o	S_w	S_c	A_o	A_w	A_c
−5	49	19	−7	111	28	−36	−92	−20	7	7	0
37	48	11	−1	−105	−24	32	−100	−23	−1	−1	0
22	−50	−11	−1	−1	0	−10	50	16	−1	−65	−16
−16	47	6	−1	−105	−23	28	76	15	−1	−65	−15
19	46	2	0	104	26	20	96	21	0	64	16
−102	−102	−29	−1	−1	0	−9	49	15	−1	−65	−16
−95	−95	−27	2	2	0	44	−84	−21	2	2	0
54	54	18	−3	−107	−25	9	67	15	−3	−67	−16

Table 2: BER in different thresholds with EC of 200 bits.

The proposed method			RHS		
G	δ	BER	G	T	BER
4	7	0.000	96	60	0.490
5	8	0.005	104	60	0.490
6	10	0.005	112	56	0.490
7	10	0.005	120	48	0.490
7	11	0.005	128	40	0.015
8	8	0.000	136	32	0.000
8	9	0.000	144	24	0.000

achieve only by setting an appropriate threshold. However, there is no such problem for the proposed method because the threshold is always 0.

4.2. Robustness against Other Attacks. This section introduces the watermarking robustness against other attacks, including AWGN with standard deviation σ_n, Gaussian filter with standard deviation σ_n equal to 1.1, median filter, and Wiener filter. Tables 3 and 4 list the BER results of image Lena for the different σ_n and different sizes of filtering mask,

Table 3: Resistance to other attacks at EC of 200 bits.

Method	AWGN (σ_n)				Gaussian filter			Median filter			Wiener filter
	10	20	30	40	$3*3$	$5*5$	$7*7$	$3*3$	$5*5$	$7*7$	$7*7$
Zeng et al.'s	0	0	0	0	0.490	0.490	0.490	0.490	0.490	0.490	0.150
Proposed	0	0	0	0	0.055	0.160	0.175	0.120	0.460	0.480	0.015

Table 4: Resistance to other attacks at EC of 500 bits.

Method	AWGN (σ_n)				Gaussian filter			Median filter			Wiener filter
	10	20	30	40	$3*3$	$5*5$	$7*7$	$3*3$	$5*5$	$7*7$	$7*7$
Zeng et al.'s	0	0	0	0	0.528	0.528	0.528	0.528	0.528	0.528	0.528
Proposed	0	0	0	0	0.132	0.270	0.270	0.214	0.492	0.482	0.026

and the PSNR is around 34 dB. Under the AWGN with different σ_n, both the two methods perform well, because it is just a simple additive noise. But as for other complicated attacks, the proposed scheme performs better than Zeng et al.'s. For the Gaussian filter and median filter, Zeng et al.'s method does not have any correct rate, our method can still maintain a certain accuracy. Even under multiplicative noise attacks, the proposed method still can yield a stable performance.

5. Conclusion

In this study, a reversible robust watermarking scheme is proposed. Different from the previous RRW methods, watermarks are embedded into the compression domain in our scheme. The reversible watermarks and robust watermarks are embedded into the coefficients of different frequency bands respectively. Meanwhile, the algorithm preferentially selects the region with complex image texture for robust watermark embedding and the smooth texture region for reversible watermark embedding. That will cause less distortion. The message can be extracted and the cover image could be recovered only if the marked image has not been attacked; otherwise, the message still could be extracted. Experiment results indicate that the proposed method can yield a quite good performance from enhancing the capacity to robustness, especially for the textural images.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (2020YFB1807500) and in part by the Fundamental Research Funds for the Central Universities (XJS210107).

References

[1] D. Zhai, C. Wang, R. Zhang, H. Cao, and F. R. Yu, "Energy-saving deployment optimization and resource management for UAV-assisted wireless sensor networks with NOMA," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6609–6623, 2022.

[2] D. Zhai, H. Li, X. Tang, R. Zhang, and H. Cao, "Joint position optimization, user association, and resource allocation for load balancing in UAV-assisted wireless networks," *Digital Communications and Networks*, 2022.

[3] J. Du, F. R. Yu, G. Lu, J. Wang, J. Jiang, and X. Chu, "MEC-Assisted immersive vr video streaming over terahertz wireless networks: a deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9517–9529, 2020.

[4] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2022.

[5] S. Mao, L. Liu, N. Zhang et al., "Reconfigurable intelligent surface-assisted secure mobile edge computing networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6647–6660, 2022.

[6] H. Guo, Y. Li, and S. Jajodia, "Chaining watermarks for detecting malicious modifications to streaming data," *Information Sciences*, vol. 177, no. 1, pp. 281–298, 2007.

[7] J. Sun, W. Wang, L. Kou et al., "A data authentication scheme for UAV ad hoc network communication," *The Journal of Supercomputing*, vol. 76, no. 6, pp. 4041–4056, 2020.

[8] T. K. Al-Shayea, C. X. Mavromoustakis, J. M. Batalla et al., *Medical Image Watermarking in Four Levels Decomposition of DWT Using Multiple Wavelets in IoT Emergence[M]Convergence of Artificial Intelligence and the Internet of Things*, Springer, Cham, 2020.

[9] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, p. 1, 2022.

[10] J. Feng, W. Zhang, Q. Pei, J. Wu, and X. Lin, "Heterogeneous computation and resource allocation for wireless powered federated edge learning systems," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3220–3233, May 2022.

[11] R. Thabit and B. Ee Khoo, "A new robust reversible watermarking method in the transform domain, the 8th international conference on robotic, vision," *Signal Processing & Power Applications*, 168, 161.

[12] D. Coltuc and J.-M. Chassery, "Distortion-free robust watermarking: a case study," *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, p. 65051N, 2007.

[13] D. Coltuc, "Towards distortion-free robust image authentication," *Journal of Physics: Conference Series*, vol. 77, no. 1, Article ID 012005, 2007.

[14] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[15] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.

[16] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: a new framework and an implementation," *IEEE Transactions on Image Processing*, vol. 15, no. 4, pp. 1042–1049, 2006.

[17] C.-C. Chang and T. D. Kieu, "A reversible data hiding scheme using complementary embedding strategy," *Information Sciences*, vol. 180, no. 16, pp. 3045–3058, 2010.

[18] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, 2004.

[19] C. Wang, X. Li, and B. Yang, "High capacity reversible image watermarking based on integer transform," *Image Processing*, vol. 217–220, 2010.

[20] F. Peng, X. Li, and B. Yang, "Adaptive reversible data hiding scheme based on integer transform," *Signal Processing*, vol. 92, no. 1, pp. 54–62, 2012.

[21] S. Weng and J. S. Pan, "Integer transform based reversible watermarking incorporating block selection," *Journal of Visual Communication and Image Representation*, vol. 35, pp. 25–35, 2016.

[22] X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction -error expansion," *Signal Processing*, vol. 93, no. 1, pp. 198–205, 2013.

[23] D. M. Thodi, J. J. Rodriguez, and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, 2007.

[24] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," *IET Information Security*, vol. 2, no. 2, pp. 35–46, 2008.

[25] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 873–882, 2011.

[26] 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.

[27] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3.4, pp. 313–336, 1996.

[28] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 4, pp. 497–509, 2008.

[29] X. T. Zeng, L. D. Ping, and X. Z. Pan, "A lossless robust data hiding scheme," *Pattern Recognition*, vol. 43, no. 4, pp. 1656–1667, 2010.

[30] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 8, pp. 1061–1070, 2011.

[31] L. An, X. Gao, Y. Yuan, D. Tao, C. Deng, and F. Ji, "Content adaptive reliable robust lossless data embedding," *Neurocomputing*, vol. 79, pp. 1–11, 2012.