Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6694729, 15 pages
https://doi.org/10.1155/2021/6694729

Research Article

Data Security Storage Method for Power Distribution Internet of Things in Cyber-Physical Energy Systems

Jiayong Zhong and Xiaofu Xiong

State Key Laboratory of Power Transmission Equipment & System Security and New Technology (Chongqing University), China

Correspondence should be addressed to Jiayong Zhong; 20071102080@cqu.edu.cn

Received 30 October 2020; Revised 4 December 2020; Accepted 15 December 2020; Published 5 January 2021

Academic Editor: Mohammad R. Khosravi

The existing cloud storage methods cannot meet the delay requirements of intelligent devices in the power distribution Internet of Things (IoT), and it is difficult to ensure the data security in the complex network environment. Therefore, a data Security Storage method for the power distribution IoT is proposed. Firstly, based on the "cloud tube edge end" power distribution IoT structure, a cloud edge collaborative centralized distributed joint control mode is proposed, which makes full use of the collaborative advantages of cloud computing and edge computing to meet the real-time requirements. Then, a distributed data storage method based on the Kademlia algorithm is proposed, and the homomorphic encryption and secret sharing algorithm are used to store the data in the cloud as ciphertext and perform data query directly on the ciphertext. Finally, considering the heterogeneity of edge nodes, the security protection model of edge nodes based on noncooperative differential game is established, and the algorithm of optimal defense strategy of edge nodes is designed to ensure the security of edge nodes. The experimental results show that the proposed method obtained excellent query performance, and the ability to resist network attacks is better than other comparison methods. It can reduce the data storage and query delay and ensure the data security of the system.

1. Introduction

As the core manifestation of the application in the field of power Internet of Things (IoT), the power distribution IoT in cyber-physical energy systems is responsible for the visual perception of the state of the distribution network, the IoT to manage and control the distribution network equipment, the opening of the distribution service capabilities, and the sharing of distribution network data [1]. On the one hand, a large number of sensor and complex communication networks were used to turn the distribution network into a multidimensional and heterogeneous complex network capable of real-time perception, dynamic control, and information query by the power distribution IoT in cyber-physical energy systems; its massive external data can affect the distribution network. The control decision of the electrical system increases the complexity of operation and control [2, 3].

With the development of cloud computing technology, more and more power grid companies are accustomed to using various services provided by cloud service providers to meet the needs of power business application development and data storage [4]. In recent years, applications such as IoT, artificial intelligence, and big data have also developed rapidly. However, because cloud computing is located at the upper layer of the network and is far away from the actual physical equipment, it cannot achieve good support for low-latency power business applications and cannot meet certain requirements. Some power applications must rely on local equipment to perform a large number of calculations [5, 6]. Edge computing allows devices to complete data collection and preprocessing in the local network by deploying edge computing devices close to the data source, thereby overcoming the problems of low processing speed and large transmission delay for massive native data in cloud computing [7]. The edge computing nodes in the power distribution IoT use edge intelligent terminals to complete the collection, aggregation, and model processing of IoT device data to meet the response requirements of low-latency applications [8].

The cooperation of cloud edge collaboration overcomes the problems of cloud computing for distributed data collection, transmission delay, and data analysis efficiency [9]. And in the power distribution IoT, the edge intelligent terminals are deployed near the power grid line data source to provide computing services, which has the advantages of real-time and efficiency [10, 11]. However, with the introduction of edge computing, a large amount of data is stored in the local edge intelligent terminal, which brings serious security risks. Moreover, edge computing involves the interaction between the edge intelligent terminal and the downstream terminal device, the interaction between the edge intelligent terminal and the upstream cloud platform, the interaction between the edge intelligent terminal, etc., which will lead to the security threats from the end devices, the edge intelligent terminal itself, the edge network infrastructure, and the cloud platform [12, 13]. At the same time, the development of the network security standards of the power distribution IoT is uneven, resulting in greater difficulties in protecting data storage from external threats [14]. Therefore, it is meaningful to study the security protection of the distributed storage of the power distribution IoT to ensure the safety and reliability of the grid data.

2. Related Research

In the existing research methods, most methods are based on the topology model to establish the power grid information model by centralized storage, which is mainly divided into three types based on the adjacency matrix, the correlation characteristic matrix [15], and the graph theory [16]. Ref. [17] studies the storage architecture of mobile edge computing, which explores the potential of mobile edge computing to enhance data analysis of IoT applications. The experiment results show that the data security and computing efficiency were achieved. Ref. [18] proposed an efficient and secure encrypted search architecture based on mobile cloud storage. In architecture, mobile devices can offload intensive computing tasks to edge servers to improve efficiency. In addition, in order to protect data security, the correlation between query keywords and search results from the cloud is hidden to reduce the information acquisition of untrusted cloud. However, the architecture model has the defect of a large amount of data, which requires a lot of memory resources for calculation, which is not suitable for a large power grid [19]. Ref. [20] proposed a nontechnical loss (NTL) detection scheme supported by edge computing and big data analysis tools to solve the problem of big data NTL fraud detection in a smart grid, providing experience for the development of big data security solutions in smart grid. However, it only focuses on the topological connection relationship, and the data interaction relationship is over conceptualized and unable to correspond with the actual system components [21]. Ref. [22] proposed a data exchange architecture for energy Internet that takes into account edge computing efficiency and data security. In this architecture, edge computing is applied to solve the challenges related to data exchange and data security at the same time. However, due to the lack of topological structure caused by the complete formulation, the model cannot reflect the actual structural characteristics of the system.

Due to the large amount of data, the above control mode model is difficult to ensure the real-time control and information security, and the energy consumption of cloud computing is too high [23]. Based on the concept of edge computing, Ref. [24] proposes an efficient and privacy-preserving data download scheme for VANET. By analyzing the encrypted requests from nearby vehicles, the road-side unit can find popular data without sacrificing the privacy of its download request. The results of the security analysis show that the scheme can resist various security attacks and improve the download efficiency of the system. Ref. [25] proposed an effective ciphertext policy attribute based on the encryption scheme, which introduced the concept of partial hiding policy to protect private information in the access policy. From the perspective of distributed control, Ref. [26] constructs a cloud edge collaborative computing framework and proposes data token and energy token inspired by blockchain and security solutions for protecting vehicle data interaction. However, the introduction of edge computing into the cyber-physical system storage data security modeling is still lack of research. Based on the existing research, this paper constructs a cloud edge collaborative data processing structure model of the power distribution IoT based on the existing research and studies the data Security Storage methods of the Distribution IoT.

Aiming at the data security problem in cloud edge collaboration of power distribution IoT in cyber-physical energy systems, a data Security Storage method is proposed. The innovation of the proposed method is as follows:

(1) In view of the fact that the distribution cloud master station cannot meet the demand of massive terminal data request delay, the proposed method is based on the "cloud-tube-edge-end" power distribution IoT structure in cyber-physical energy systems and proposes a cloud edge collaborative control mode, which makes full use of the coordination of cloud and edge computing to improve the efficiency

(2) Aiming at improving the data storage security of the edge intelligent terminal, a distributed data storage method based on the Kademlia algorithm is proposed, and the improved homomorphic encryption and secret sharing algorithm are used to make all the edge intelligent terminal data stored and queried in the ciphertext

(3) Because of the heterogeneous and distributed characteristics of edge intelligent terminals, it is easier for network attackers to launch malicious attacks. Therefore, the proposed method establishes an intrusion prevention model of edge intelligent terminals based on the stochastic differential game, which provides the optimal defense strategy for each edge intelligent

terminal, so as to ensure the data security of power distribution IoT

3. System Architecture

3.1. Hierarchical Structure of Power Distribution IoT in Cyber-Physical Energy Systems. The power distribution IoT is the embodiment of the application of the power IoT in the field of distribution. It undertakes the functions of perceiving the status of the visual distribution network, controlling the distribution network equipment, opening the service ability of the distribution network, and sharing the data of the distribution network, so as to realize the internal support of the grid operation, customer service, enterprise operation, and other businesses, and the external business supports the resource commercial operation, energy finance, comprehensive energy service, and virtual power plant and other businesses [27]. The power distribution IoT overall structure in cyber-physical energy systems is shown in Figure 1.

The structure of power distribution IoT can be divided into four core levels of "cloud-management-edge-device," and each level is described as follows.

(1) *Cloud*: as the distribution cloud master station platform, it adopts cloud computing, big data, artificial intelligence, and other technologies to realize the comprehensive cloud and microservice of the master station under the IoT architecture. The first mock exam platform of distribution cloud can satisfy the business requirements of massive devices such as plug and play, data integration, and cloud collaboration. It supports the business requirements such as low voltage unified model management, plug and play, data cloud synchronization, and IoT management. The main station needs to have flexible Internet of Things cloud service and cloud edge collaboration ability, which could meet the requirements of rapid response, dynamic allocation of resources, intensive operation, and maintenance of the system at the same time. "Cloud" layer includes the platform as a service, infrastructure as a service, and software as a service layer

(2) *Management*: as a data transmission channel of "cloud," "edge," and "end," it is used to complete the efficient transmission of massive information in the power grid. It can be divided into two main parts: remote communication network and local communication network, where the remote communication network provides the data communication channel between the distribution cloud master station and the edge intelligent terminal, and the local communication network provides the data communication channel between the edge intelligent terminal and the terminal unit

(3) *Edge*: the edge intelligent terminal, with "edge cloud, cloud gateway" as the main landing form, and "cloud edge collaboration, edge intelligence" as the core feature, which is an open platform for data aggregation and computing. In the power distribution IoT system structure, the edge intelligent terminal is the carrier and key link of terminal data self-organization and end cloud business self-coordination, which realizes the decoupling of terminal hardware and software functions. For the "end" end, the data exchange and intelligent sensing equipment are used to complete the edge end collaboration to achieve full data acquisition, full perception, and full control; for the "cloud" end, the edge intelligent terminal and the distribution cloud master station interact in real-time and full-duplex mode with key operation data to complete edge cloud collaboration, give full play to the expertise of cloud computing and edge computing, and realize reasonable division of labor

(4) *Devices*: terminal device (various types of sensor units), as the sensing layer and execution layer in the power distribution IoT architecture; "end" refers to the source of basic data such as operation status, environmental status, and equipment environmental status of the distribution network to "edge" or "cloud," and the terminal for executing decision-making command or local control

3.2. Cloud Edge Collaboration for Power Distribution IoT in Cyber-Physical Energy Systems. Different from the centralized storage structure where the distribution cloud master station completes all the computing tasks, the edge intelligent terminal is added to the edge side of the cloud edge collaborative structure near the data source, as shown in Figure 2. The distributed collaboration theory divides the distribution network terminal devices and the edge intelligent terminals into multiple distributed collaboration according to the region and operation state. All the power and information components in each distributed collaboration and the edge intelligent terminal jointly constitute a distributed open-edge service platform integrating the core functions of the network, storage, computing, and application, providing the edge intelligent services in the regional distributed collaboration, shorten the information transmission link, and realize the communication and regional interconnection with the cloud computing center through the backbone network [28].

The control mode of cloud edge collaboration can make full use of the collaborative advantages of cloud computing and edge computing, realize unified scheduling, and meet the security and real-time requirements [29, 30]. The business in the local area is uploaded to the edge intelligent terminal after the data is collected by the terminal devices, which is executed locally by the edge intelligent terminal or completed by the cooperation of multiple edge intelligent terminals through the local area networks, such as plug and play application and application localization management. The data information of the edge intelligent terminal and the terminal devices is stored in the edge intelligent terminal in modular form. Some advanced applications, such as distribution network

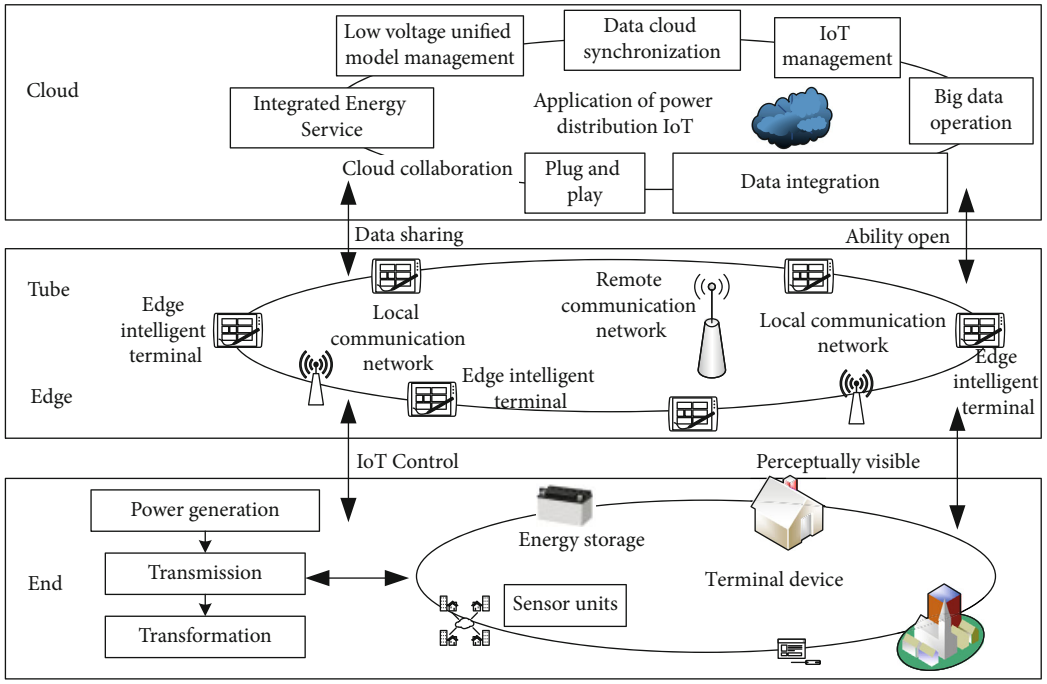

Figure 1: Overall structure of power distribution IoT in cyber-physical energy systems.

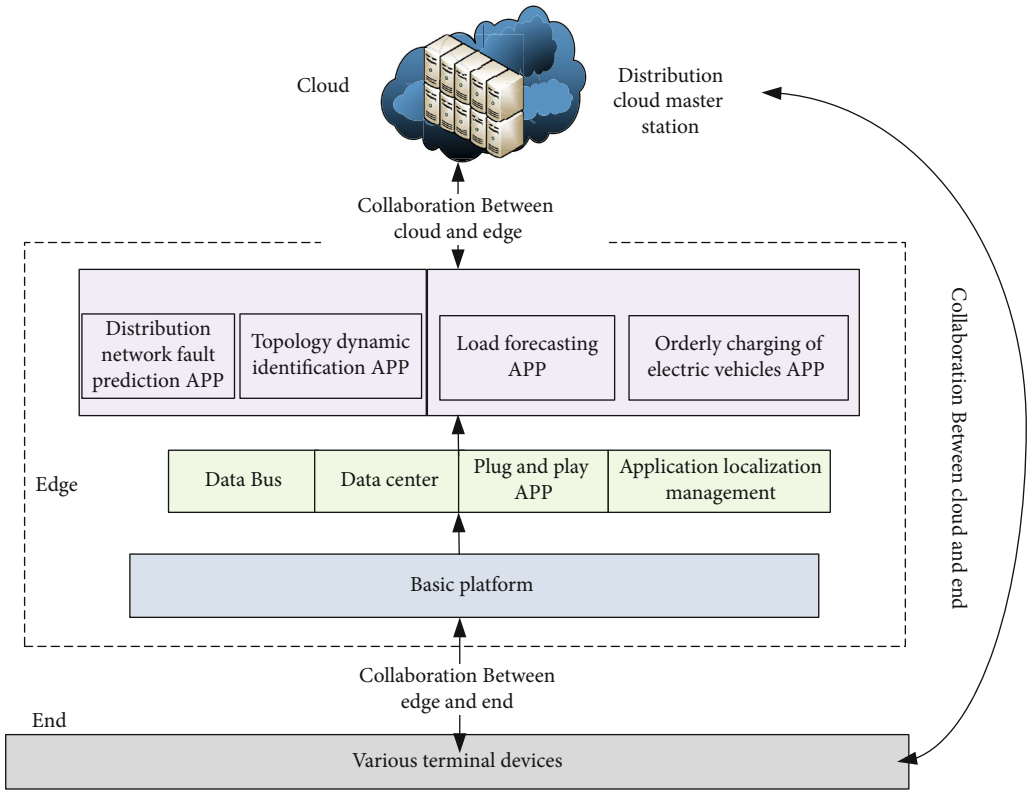

Figure 2: The structure of centralized-distributed joint control based on cloud-edge collaboration.

fault prediction, topology dynamic identification, orderly charging of electric vehicles, and load forecasting, are completed by the edge intelligent terminal and the distribution cloud master station. Among them, the edge intelligent terminal completes the optimization calculation, and then, the distribution cloud master station sends control commands to the edge intelligent terminal for partition execution [31].

4. Data Security Storage Method

4.1. Data Storage and Query Model

4.1.1. Data Storage Model. Firstly, it is necessary to create a database on the edge intelligent terminal, that is, the client application, and randomly generate two large prime numbers $p1$ and $p2$ (usually used to use prime numbers with more than 512 bits, such as 1024 bits), to obtain the product n of the two, namely:

$$\varphi(n) = (p1 - 1)(p2 - 1), \tag{1}$$

A random number p also need to be generated to represent a positive integer coprime with n. Then, a new table T is created in the distribution cloud master station database, a field column A is created, and a column key named $ck_A = \langle x_A, y_A \rangle$, x_A, and y_A are randomly generated, but $x_A, y_A < n$ is required. In addition, each row is defined as $r_i (r_i > 0)$ which is stored separately in a column named *row-id*, and the *row-id* requires additional encryption, and the value of the column can be encrypted using an improved homomorphic encryption algorithm (defined as $r_i (r_i > 0)$) that supports addition. In this way, table T has two columns (*row-id*, A). The edge intelligent terminal only needs to store $p1$, $p2$, and ck_A, and the actual value of the table is stored in the distribution cloud master station database.

In summary, the data model is built in the integer field for operation. After getting the plaintext data V to be inserted, V needs to be encrypted by ck_A and r_i. In other words, V_{key} is generated by ck_A andr_i, and V_{key} is generated as follows:

$$V_{\text{key}} = g(r, (x, y)) = xp^{ry \bmod \varphi(n)} \bmod n, \tag{2}$$

Then, V_e is generated by V_{key} and plaintext V. V_e is the encrypted ciphertext value of the data:

$$V_e = E\left(V, V_{\text{key}}\right) = VV_{\text{key}}^{-1} \bmod n, \tag{3}$$

where V_{key}^{-1} is the modular inverse of V_{key}.

The generated V_e is stored in the distribution cloud master station database, and V_{key} as the intermediate value of calculation does not need to be stored, because the value of V_{key} can be recovered through ck_A and r_i. V_{key} and V_{key} values are needed to decrypt the data when the value needs to be decrypted:

$$V = D\left(V_e, V_{\text{key}}\right) = V_e V_{\text{key}} \bmod n. \tag{4}$$

For the whole database, the edge intelligent terminal only needs to save two positive integers n and p, while for table T and column A in the database, the edge intelligent terminal only needs to save the column key ck_A of the column. In the distribution cloud master station database, the encrypted line number $E^+(r)$ and the ciphertext value A_e of the data are saved in the database. Compared with other encryption cloud data storage models, this model does not need to occupy additional database space of the distribution cloud master station to store metadata for data repair [32].

4.1.2. Query Model. The database system SHAMC can directly execute ciphertext SQL queries on the data tables created by the database layer of the power distribution cloud master station, which all rely on the improved homomorphic encryption algorithm of the model. The query algorithm is jointly implemented by the protocol stack designed and stored on the edge intelligent terminal and the power distribution cloud master station database [33, 34]. These protocols are designed and written in the User-Defined Function (UDF) of the edge intelligent terminal of the database management software (DMS).

SHAMC supports most of the operators of SQL statements and can pass all the statement tests of TPC-H. Taking the commonly used multiplication operators as an example, we will introduce the process of implementing encrypted queries.

Assuming that the data table T has two encrypted columns, column A and column B, the calculation result $A \times B$ is to be obtained. A, B keys $ck_A = \langle x_A, y_A \rangle$ and $ck_B = \langle x_B, y_B \rangle$. Assuming that the result column is column C, the column key of column C is $ck_C = \langle x_C, y_C \rangle$. To get the value of C through the values of A and B, you need to calculate C_e and ck_C. Specifically, execute the protocol edge intelligent terminal protocol *mul_cal_x* and *mul_cal_y*, get ck_c:

$$ck_C = \langle x_C, y_C \rangle = \langle x_A y_B, x_A + y_B \rangle. \tag{5}$$

Then, execute the protocol *mul_cal_*c_e on the database of the power distribution cloud master station to get c_e:

$$C_e = A_e B_e \bmod n. \tag{6}$$

can be pushed:

$$C_{\text{key}} = x_c \cdot p^{\text{ryc}} = x_A \cdot x_B \cdot p^{r(x_A + y_B)} = A_{\text{key}} \cdot B_{\text{key}} (\bmod n). \tag{7}$$

Therefore, it can be proved:

$$\begin{aligned} C &= C_e \cdot C_{\text{key}} = A_e \cdot B_e \cdot C_{\text{key}} \\ &= A \cdot A_{\text{key}}^{-1} \cdot B \cdot B_{\text{key}}^{-1} \cdot A_{\text{key}} \cdot B_{\text{key}} = A \cdot B. \end{aligned} \tag{8}$$

4.2. Data Safe Storage.

In order to avoid the problems caused by the centralized storage system, a distributed data storage system is designed based on the Kademlia algorithm by using the edge computing architecture. The Kademlia algorithm has the characteristics of simplicity, flexibility, and security. Assign a randomly generated 160-bit node identity (ID, identity) to each edge intelligent terminal joining the Kademlia network. The 160-bit hash value of the encrypted data block is used as the number, called the key, and the encrypted data block itself is used as the value, and then, the data block is stored in the form of key-value pairs on several edge intelligent terminals with ID values similar to the key. The maximum number of nodes that can be accommodated in the Kademlia network is 2,160, and its storage capacity far

exceeds the number of devices required in the actual network, thus meeting the scalability requirements of large-scale IoT applications [35].

Each edge intelligent terminal in the distributed storage system only stores a part of the encrypted data and does not store a complete data ledger. In addition, the state information of the edge intelligent terminal is stored in each node through the K-bucket mechanism. Kademlia algorithm calculates the distance between nodes through exclusive OR operation. The distributed storage structure based on edge computing is shown in Figure 3. Each edge intelligent terminal has a 160-layer K-bucket mechanism table.

For K-bucket i, the edge intelligent terminal stores the status messages of k nodes whose distance is $[2^{i-1}, 2^i)$. These messages include node ID, Internet Protocol (IP) address, and access port. k is a system-level constant, which can be set to 8 according to the dynamic setting of the storage system, such as the Kademlia algorithm used in the bit stream. The state storage method based on the K-bucket mechanism makes n edge intelligent terminals need lg$n$ queries at most to find the target information.

The distributed storage architecture based on edge computing effectively avoids the two common problems of traditional distributed systems. Firstly, the entry/exit of nodes in a distributed system is very frequent. When the node status changes, the entire network will update the broadcast address and synchronize the nodes, which leads to network congestion and greatly reduces the storage and search efficiency [36]. In the proposed secure storage solution, each node only maintains some of the messages of edge intelligent terminals, so that the impact on the entire network is minimized when any node changes its state. Then, in the traditional architecture, each node maintains the status information of the entire network. Once a node is attacked or deliberately committed evil, the status information of all nodes will be leaked. The Kademlia algorithm is used to provide partition fault tolerance for the storage system, which greatly reduces the risk of information leakage.

4.3. Data Defense Model. Edge intelligent terminals process and store data, and the separation of ownership and control rights causes edge intelligent terminals to lose physical control of their data. A large number of edge intelligent terminals, local deployment, and wide geographic distribution make it easier and more efficient for intruders in this computing mode to launch denial of service attacks [37]. If effective detection and defense mechanisms are not deployed on edge smart terminals, malicious intruders can launch attacks by consuming limited resources of computing and bandwidth. Meanwhile, it also can forge false data centers, deceive edge smart terminals and obtain users sensitive data or even tty to control the devices.

In order to establish a defense mechanism suitable for edge intelligent terminals, in this section, modeling and analysis of the interaction behavior between attack nodes and edge nodes by noncooperative differential game theory are taken into account, where the heterogeneity of distribution IoT and the ability of edge nodes are able to respond detection and defense functions autonomously.

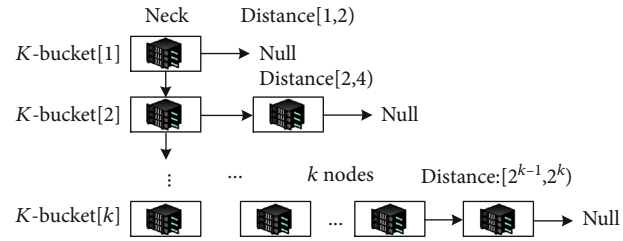

Figure 3: Distributed storage architecture based on edge computing.

In the environment of edge computing, the number of edge intelligent terminals is recorded as N, and each edge intelligent terminal is deployed with an intrusion prevention system, so that $x(t)$ is the number of intruders at t time, and represents the defense strength of the intrusion prevention system deployed at the edge intelligent terminal i at time t, where $i = 1, 2, \cdots, N$. Let $v(t)$ denote the attack frequency of the intruder at t time. When the intruder attacks any edge intelligent terminal maliciously, the change process of the number is related to the defense strength of the edge intelligent terminal's intrusion prevention system and the current attack strength. Therefore, the change process of the number of invaders can be described by the following equations:

$$\begin{cases} \dfrac{dx(t)}{dt} = ax(t) - b_i u_i(t) + cv(t), \\ x(t_0) = x_0 > 0, \end{cases} \tag{9}$$

where a represents that when the intruder's trajectory is not detected, the intruder increases the growth rate of its number by attacking the edge intelligent terminal, b_i represents that the intrusion prevention system deployed on the edge intelligent terminal successfully detects and blocks the intruder probability, c represents the probability of an intruder successfully attacking under the action of the intrusion prevention system, t_0 represents the initial time of the game, and x_0 represents the initial number of intruders.

When it is attacked maliciously in the game process, the edge intelligent terminal can detect and block the behavior of malicious intruders by deploying and responding to the intrusion prevention system. The edge nodes also could prevent the attacks by reducing the attack intensity and the number of intruders minimizing the resource consumption cost caused by its own defense measures. In the process of edge intelligent terminal being attacked, with the increase of the number and frequency of intruders, the cost of deploying defense system and reducing the number of intruders are $\alpha_i u_i^2(t)$ and $\varepsilon_i x(t)$, respectively, where α_i is the unit cost of edge intelligent terminal i, and ε_i is the unit cost of reducing the number of intruders to respond to the defense system.

In addition, the cost of computing resources consumed by each edge intelligent terminal to successfully resist malicious attacks can be expressed as a function of attack frequency, i.e., $\beta v(t) u_i(t)$, where β is the unit cost of computing resource consumption. The resource consumption caused by a false alarm attack of the intrusion prevention

system is $\chi_i u_i(t)$, and χ_i represents the unit cost caused by false alarm attack.

For any edge intelligent terminal i, try to minimize its computing resource cost during the game. According to the above analysis, the total cost function of the edge intelligent terminal i deployed with the intrusion prevention system on the game time $[t_0, T]$ is expressed as:

$$J_i^D = \min_{u_i(t)} \int_{t_0}^{T} (u_i(t)(\alpha_i u_i(t) + \chi_i) + \beta v(t) u_i(t) + \varepsilon_i x(t)) \exp[-r(t-t_0)]dt + q_i(x(T)) \exp[-r(T-t_0)], \tag{10}$$

where T represents the time when the game ends, r represents the ratio of the future cost of the edge smart terminal to the current cost, and $q_i(x(T)) \exp[-r(T-t_0)]$ represents the cost function of the edge smart terminal at the end of the game.

In the attack process, the intruder tries to achieve the maximum damage to the defense system by increase the attack intensity, which is conducted by maximizing the attack frequency and increasing the number of intruders. Therefore, the total cost function of the intruder in the game time $[t_0, T]$ is expressed as:

$$J^A = \min_{v(t)} \int_{t_0}^{T} \left(\eta v^2(t) + \kappa u_i(t) v(t) + \lambda x(t)\right) \exp[-r(t-t_0)]dt + q_i(x(T)) \exp[-r(T-t_0)]. \tag{11}$$

For the edge intelligent terminal, if there is a continuous differentiable function $U^i(t,x)$: $[t_0,\infty] \times R \to R$ for any edge intelligent terminal i, it satisfies the Isaacs Bellman equation:

$$U^i(t,x) = \exp[-r(t-t_0)] \int_0^{\infty} \left(\alpha_i [\phi_i^*(t,x)]^2 + \beta v(t) \phi_i^*(t,x) + \chi_i \phi_i^*(t,x) + \varepsilon_i x(t)\right) \times \exp[-r(t-t_0)]dt. \tag{12}$$

Then, the strategy set $\{u_i^*(t) = \phi_i^*(t,x) | i = 1, 2, \cdots, N\}$ is the feedback Nash equilibrium solution.

According to the Nash equilibrium solution process, in the infinite time domain, the optimal defense strategy of the edge intelligent terminal i is $u^*(t)$:

$$u^*(t) = \frac{(2\eta b_i \varepsilon_i + \beta c \lambda) \exp[r(t-t_0)]}{(4\alpha_i \eta - \beta\kappa)(r-a)} - \frac{2\eta\chi_i}{4\alpha_i\eta - \beta\kappa}. \tag{13}$$

Similarly, the optimal strategy for the intruder i is $v^*(t)$:

$$v^*(t) = \frac{-\varepsilon_i c \exp[r(t-t_0)]}{2\eta r - a} - \frac{2\eta\chi_i\kappa(r-a) + (\varepsilon_i\kappa\beta c + 2\eta b_i \kappa\lambda) \exp[r(t-t_0)]}{2\eta(4\alpha_i\eta - \beta\kappa)(r-a)}. \tag{14}$$

According to the above analysis, the edge intelligent terminal and the intruder adopt stochastic differential game modeling, and the optimal strategies in the finite and infinite time domain are obtained according to the equilibrium solution so that each edge intelligent terminal and intruder can consider the resources maximize revenue under limited circumstances. The data security preserving model of edge intelligent terminal based on the stochastic differential game in the edge computing environment is shown in Algorithm 1.

4.4. Cloud Edge Collaborative Storage Security Defense. The proposed cloud edge collaborative storage security defense scheme includes four stages: preparation stage, transmission stage, sharing stage, and retrieval stage.

(1) *Preparation stage*: each edge intelligent terminal inputs a security parameter 1^k to generate public-private key (PK, SK). The initialization algorithm is as follows:

$$\begin{aligned} (\mathrm{PK}_{\mathrm{PKE}}, \mathrm{SK}_{\mathrm{PKE}}) &\leftarrow \mathrm{PKE.Setup}\left(1^k\right), \\ (\mathrm{PK}_{\mathrm{PKES}}, \mathrm{SK}_{\mathrm{PKES}}) &\leftarrow \mathrm{PKES.Setup}\left(1^k\right), \\ (\mathrm{PK}_{\mathrm{DS}}, \mathrm{SK}_{\mathrm{DS}}) &\leftarrow \mathrm{DS.Setup}\left(1^k\right). \end{aligned} \tag{15}$$

The edge intelligent terminal manages the private key SK by itself and then sends the corresponding public key PK to the CA for registration. CA will use its private key $\mathrm{SK}_{\mathrm{DS}}^{\mathrm{CA}}$ to sign the identity information of the edge intelligent terminal and the public key PK of the edge intelligent terminal, so as to generate the digital certificate Cert of the edge intelligent terminal. Finally, CA sends the generated digital certificate Cert to the edge intelligent terminal.

(2) *Transmission stage*: the data sending terminal device logs into a similar edge intelligent terminal, extracts some keywords W for the query from the data F it wants to store in the distribution cloud master station, and then uses its own private key $\mathrm{SK}_{\mathrm{DS}}^{O}$ to generate a digital signature sign for the data F

$$\mathrm{sign} \leftarrow \mathrm{DS.Sig}\left(\mathrm{SK}_{\mathrm{DS}}^{O}, F\right). \tag{16}$$

Data sending terminal device sends data F, keyword W, authorized terminal device list U, digital signature sign, and its digital certificate Cert^O to edge intelligent terminal

Pseudocode of edge node oriented security defense algorithm
Input: number of nodes N
Begin
1. The security defense model of stochastic differential game is established: $\begin{cases} dx(t)/dt = ax(t) - b_i u_i(t) + cv(t), \\ x(t_0) = x_0 > 0. \end{cases}$
2. Set parameters according to network conditions a, b_i, c, α_i, ε_i, η, κ, λ, r
3. **For** $t = 0$ to T
4. Nash equilibrium method is used to calculate the game model, and the optimal strategy is obtained:
$u^*(t) = (2\eta b_i \varepsilon_i + \beta c\lambda) \exp[r(t-t_0)]/(4\alpha_i\eta - \beta\kappa)(r-a) - 2\eta\chi_i/4\alpha_i\eta - \beta\kappa$,
$v^*(t) = -\varepsilon_i c \exp[r(t-t_0)]/2\eta r - a - 2\eta\chi_i\kappa(r-a) + (\varepsilon_i\kappa\beta c + 2\eta b_i\kappa\lambda) \exp[r(t-t_0)]/2\eta(4\alpha_i\eta - \beta\kappa)(r-a)$.
5. **End for**
6. According to the equilibrium solution structure, the number of intruders is analyzed.
End

Algorithm 1:

through a secure channel. The edge intelligent terminal will generate a unique symmetric key K according to the identifier ID of each data file after receiving the data sent by the data sending terminal device.

$$K \leftarrow \mathrm{SE.Setup}\left(1^k\right). \tag{17}$$

The edge intelligent terminal uses a symmetric key K to encrypt each data file F to generate data ciphertext C_{SE}.

$$C_{\mathrm{SE}} \leftarrow \mathrm{SE.Enc}(K, F). \tag{18}$$

The edge intelligent terminal obtains the certificates $\{\mathrm{Cert}^R | R \in U\}$ of all authorized terminal devices from CA and obtains the public key $\{PK^R_{PKE}, PK^R_{PEKS}, PK^R_{DS} | R \in U\}$ of all authorized edge intelligent terminals and encrypts symmetric key K and keyword W with $\mathrm{PK}^R_{\mathrm{PKE}}$ and $\mathrm{PK}^R_{\mathrm{PEKS}}$, respectively, to generate symmetric key ciphertext C^R_{PKE} and public key searchable ciphertext $C^{R,W}_{\mathrm{PKES}}$.

$$\begin{aligned} C^R_{\mathrm{PKE}} &\leftarrow \mathrm{PKE.Enc}\left(\mathrm{PK}^R_{\mathrm{PKE}}, K\right), \\ C^{R,W}_{\mathrm{PEKS}} &\leftarrow \mathrm{PEKS.Enc}\left(PK^R_{\mathrm{PEKS}}, W\right). \end{aligned} \tag{19}$$

The edge intelligent terminal uploads data ciphertext C_{SE}, symmetric key ciphertext C^R_{PKE}, public key searchable ciphertext $C^{R,W}_{\mathrm{PKES}}$, digital signature sign of data, and the digital certificate Cert^O of data sending terminal device to distribution cloud master station.

(1) *Sharing stage*: an authorized data receiving terminal device logs in to a neighboring edge intelligent terminal, and a sharing request is submitted to the edge intelligent terminal. The edge intelligent terminal forwards the sharing request to the distribution cloud master station, and the distribution cloud master station returns all data ciphertext C_{SE}, symmetric key ciphertext C^R_{PKE}, the digital signature sign of data, and digital certificate Cert^O of data sending terminal device to the edge intelligent terminal

The edge intelligent terminal obtains the public key $\mathrm{PK}^O_{\mathrm{DS}}$ from the digital certificate Cert^O of the data sending terminal device and sends the symmetric key ciphertext C^R_{PKE} to the authorized data receiving terminal device. The authorized data receiving terminal device uses its own private key $\mathrm{SK}^R_{\mathrm{PKE}}$ to decrypt symmetric key ciphertext C^R_{PKE} and obtain symmetric key K.

$$K \leftarrow \mathrm{PKE.Dec}\left(\mathrm{SK}^R_{\mathrm{PKE}}, C^R_{\mathrm{PKE}}\right). \tag{20}$$

The authorized data receiving terminal device returns the symmetric key K to the edge intelligent terminal through the secure channel, and the edge intelligent terminal uses K to decrypt data ciphertext C_{SE} to obtain plaintext F.

$$F \leftarrow \mathrm{SE.Dec}(K, C_{\mathrm{SE}}). \tag{21}$$

The edge intelligent terminal will return the integrity verified data F to the authorized data receiving terminal device through the secure channel.

(2) *Retrieval stage*: an authorized data receiving terminal device logs in to a neighboring edge intelligent terminal and uses its own private key $\mathrm{SK}^R_{\mathrm{PEKS}}$ to generate a search trapdoor T_W for the keyword W to be queried

$$T_W \leftarrow \mathrm{PEKS.Tra}\left(\mathrm{SK}^R_{\mathrm{PEKS}}, W\right). \tag{22}$$

The data receiving terminal device sends the retrieval request of T_W and its digital certificate Cert^R to the edge intelligent terminal, which forwards the retrieval request to the distribution cloud master station. The distribution cloud master station obtains the public key $\mathrm{PK}^R_{\mathrm{PEKS}}$ of the authorized data receiving terminal device from the digital certificate Cert^R of the authorized data receiving terminal device, and uses PK^R_{PEKS} and T_W to retrieve the matched public key

searchable ciphertext set ψ_{PEKS}^{R} generated by the data sending terminal device for the authorized data receiving terminal device, and searchable ciphertext ψ_{W} can be retrieved.

$$\psi_{W} \leftarrow \mathrm{PEKS.Search}\left(\mathrm{PK}_{\mathrm{PEKS}}^{R}, \psi_{\mathrm{PEKS}}^{R}, T_{W}\right). \tag{23}$$

The distribution cloud master station will return the retrieved public key searchable ciphertext corresponding data ciphertext C_{SE}, symmetric key ciphertext C_{PKE}^{R}, digital signature of data, and digital certificate Cert^{O} of data sending terminal device to the edge intelligent terminal. After that, the data processing process between the edge intelligent terminal and the authorized data receiving terminal device is consistent with the security defense in the sharing phase.

5. Experimental Results and Analysis

The host configuration is Intel Core i3-3240 CPU@3.4GHz and 4GB of memory and using the SHAMC encryption model. My SQL 5.5 is installed at both ends as the basic database, and all encrypted query protocols are built on the UDF of MySQL. The configuration of each distribution cloud master station database is dynamically adjustable, which is convenient for comparative experiments.

In addition, six hosts are used to simulate the edge intelligent terminal, named edge1-6. Edge1-4 is equipped with Intel Xeon CPU e3-1220 (3.00 GHz) and 32 GB random access memory (RAM), while edge5-6 is equipped with Intel Xeon CPU e5620 (2.40 GHz) and 24 GB RAM; a MacBook Pro equipped with Intel Core i9-9880h and 16 GB RAM is used as the IoT consumer.

5.1. Time Delay Analysis. In order to verify the download delay performance of the proposed method, the time delay experiment is carried out. And the result is compared with the traditional cloud storage which is shown in Figure 4.

As shown in Figure 4, when the amount of data to be allocated is very small, the delay performance of cloud storage and cloud edge collaborative storage architecture is similar, because the small amount of data brings less transmission delay, and the powerful computing power of distribution cloud master station can make up for the delayed loss caused by transmission. With the continuous increase of tasks, due to the distance between the distribution cloud master station and the terminal device, a large amount of data will cause a long transmission delay, so the service response delay of cloud storage architecture increases significantly. Compared with cloud storage architecture, because the edge computing layer is close to the end devices, it can provide services for the end devices at the network edge, so the cloud edge collaborative network architecture has better delay performance.

As for the performance of the stochastic differential game algorithm in this optimization problem, it is compared with the algorithm in Ref. [17], Ref. [20], and Ref. [25], and the results are shown in Figure 5.

As can be seen from Figure 5, the delay of the four optimization algorithms increases with the increase of the task amount. However, in the case of the same amount of data, the delay of the proposed stochastic differential game algorithm is significantly less than that of other comparative algorithms, which fully proves that it has better delay optimization performance, can quickly complete information exchange, and is suitable for high standard security protection.

5.2. Comparative Analysis of Storage Capacity. The storage capacity of the edge intelligent terminal has a great impact on the data security storage performance of the power distribution IoT. In the experiment, the storage capacity of the edge intelligent terminal changes from 100 to 200 data blocks, and the network delay is 10 ms.

In order to demonstrate the performance of the proposed data security storage method, its storage capacity is compared with Ref. [17], Ref. [20], and Ref. [25]. The average acquisition delay of data resources is shown in Figure 6.

It can be seen from Figure 6 that the average acquisition delay of the distributed storage method is significantly lower than that of other storage methods. As the storage capacity of edge intelligent terminals increases, the average acquisition delay of various storage methods has decreased. This is because the greater the storage capacity of edge intelligent terminals, the more data can be stored at the network edge, thereby reducing the average acquisition delay. With the increase of the storage capacity of edge intelligent terminals, when the storage capacity is 200 data blocks, compared with 100 data blocks, the average acquisition delay of the proposed storage method is reduced by 58.3%. Ref. [17], Ref. [20], and Ref. [25] reduced by 25.5%, 22.6%, and 40.8%, respectively. It can be seen that the average acquisition delay reduction effect of the proposed storage method is the best.

5.3. Query Performance Analysis. TPC-H performance test specification is used to analyze the query performance. TPC-H performance test includes all the commonly used query operation operators and contains complex queries. Through TPC-H, it usually means that the database can support normal use and can cope with some complex business scenarios. In the experiment, all TPC-H statements can be executed correctly.

In order to compare the usability of SHAMC with other encrypted databases, two kinds of algorithm prototypes, MONOMI and crypt dB, are implemented in the experiment. In the SHAMC model, Q4, Q11, Q12, q13, Q16, and q21 are not involved in the ciphertext operation, and q13, Q15, and Q16 are not supported by the SDB, Crypt DB, and MONOMI models. Therefore, in a comprehensive consideration, some TPC-H statements are selected for verification. The execution time of the SHAMC ciphertext query TPC-H statement and plaintext query is shown in Figure 7.

As can be seen from Figure 7, SHAMC achieved much more efficiency than Crypt DB in the execution time. In the SHAMC system, most of the computation is transferred to the database layer of the distribution cloud master station. Therefore, in order to further analyze the proportion of processing time in each layer, taking Q1, Q8, q14, and q22 statements of TPC-H as an example, the comparison of the execution time of three processing processes of distribution

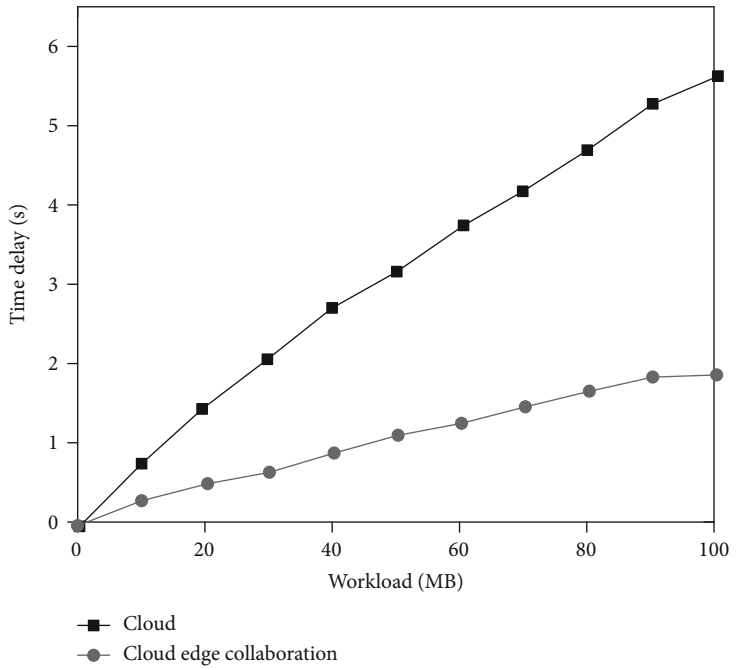

Figure 4: Delay comparison between distributed data storage and cloud storage.

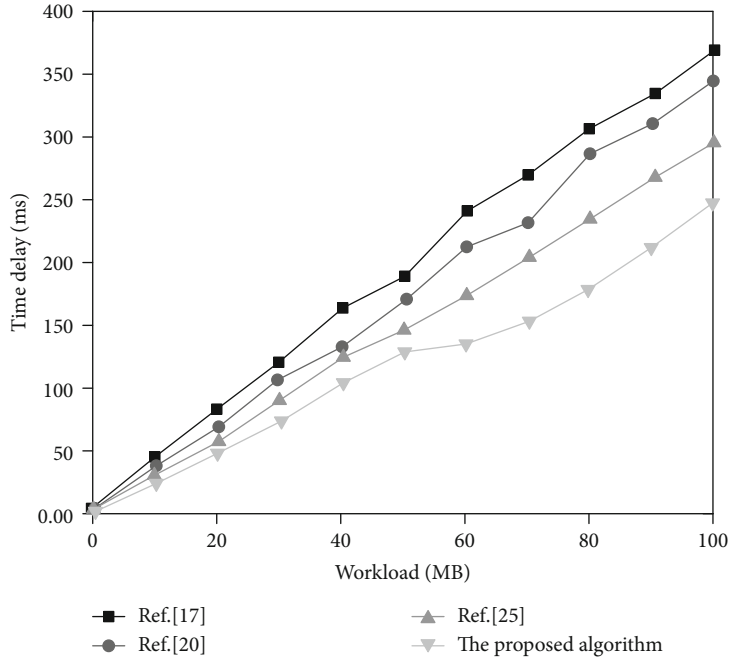

Figure 5: Delay comparison between the proposed algorithm and other algorithms.

cloud master station database layer, client application layer, and network transmission is shown in Figure 8.

As shown in Figure 8, the database protocol operation of the distribution cloud master station in the database layer of the distribution cloud takes up the vast majority of the calculation process. Compared with MONOMI, which has similar query performance, MONOMI needs to precalculate data on the client and work with the cloud to complete the query operation. In general, SHAMC has an acceptable computing overhead and transfers most of the computation to the database layer of the distribution cloud master station, which reduces the computing load of the client.

5.4. Safety Analysis. Consider that the number of edge intelligent terminals participating in the game is $N = 6$, the edge intelligent terminal and the intruder discount their future

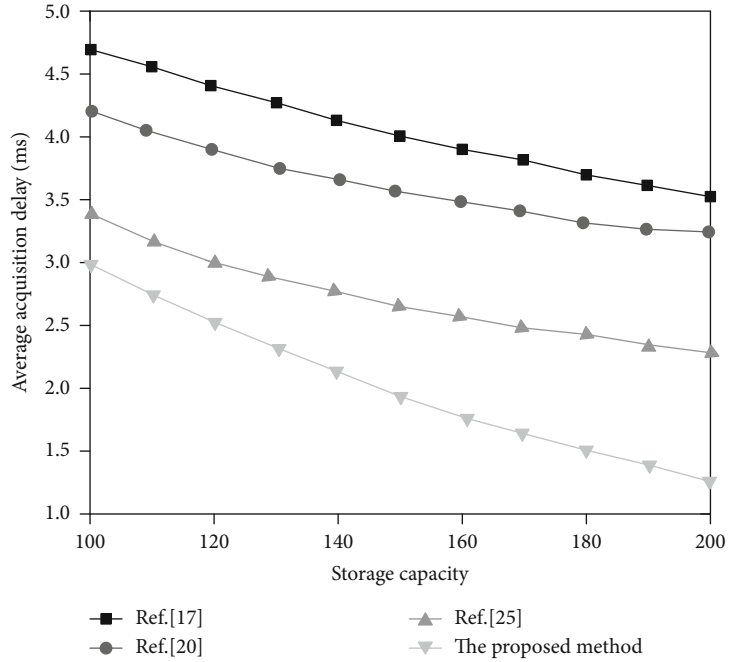

Figure 6: The effect of edge server storage capacity on cache performance.

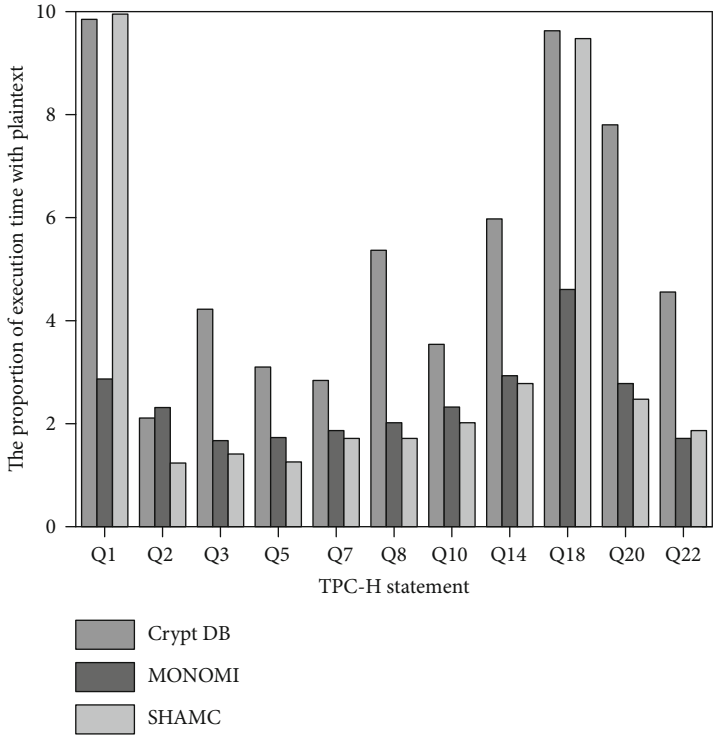

Figure 7: The ratio of execution time between the TPC-H statement and plaintext query in the encrypted database.

costs into the current cost ratio $r = 0.05$, the initial time of the game $t_0 = 0$, and the end time of $T = 20$ s.

Consider that when the probability of an intruder's successful attack is greater than or equal to 90%, the dynamic change of its attack frequency $v^*(t)$ over time is shown in Figure 9.

As can be seen from Figure 9, the attack frequency of intruders decreases with time. With the enhancement of the defense level of the edge intelligent terminal, the attack frequency of the intruder decreases gradually with the improvement of the defense level of the edge intelligent terminal. At the same time, in the process of launching

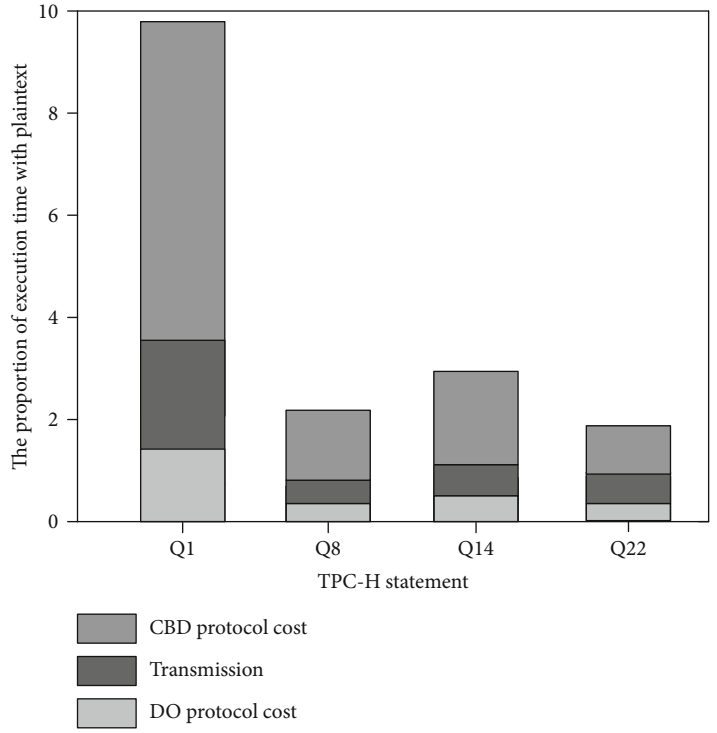

Figure 8: Comparison of execution time and plaintext query time of each process.

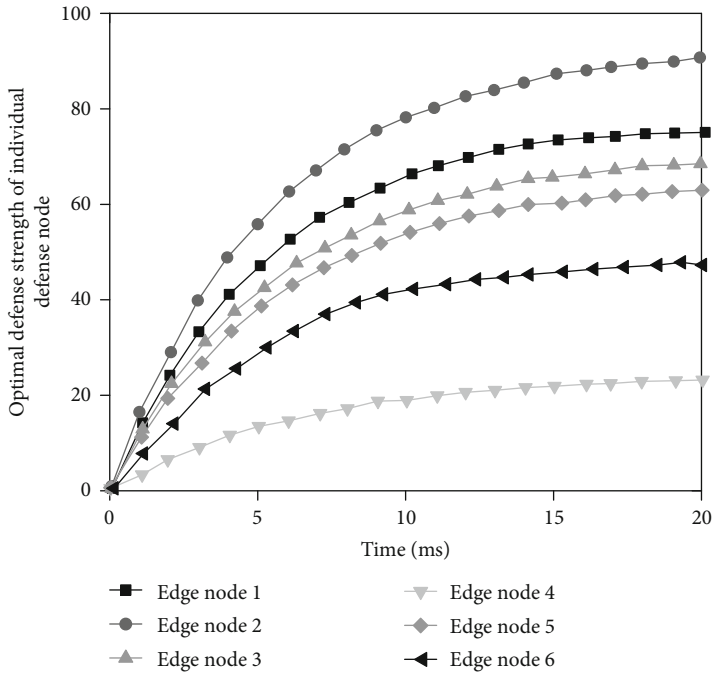

Figure 9: Change of individual optimal defense strategy of the edge node with time.

the attack, the intruder tries to maximize the illegal benefits and minimize the cost by dynamically adjusting its attack strength.

According to the above analysis, the edge intelligent terminal selects the optimal defense strategy when the intruder selects its optimal attack intensity. The change track of the number $x^*(t)$ of intruders over time is shown in Figure 10.

As shown in Figure 10, the number of intruders gradually decreases with time. Combined with the analysis in Figure 9, after $t = 10$ ms, the attack intensity of the intruders would not threaten the edge intelligent terminal security. Therefore, the proposed security protection method can effectively resist intruders while improving the security of edge smart terminals.

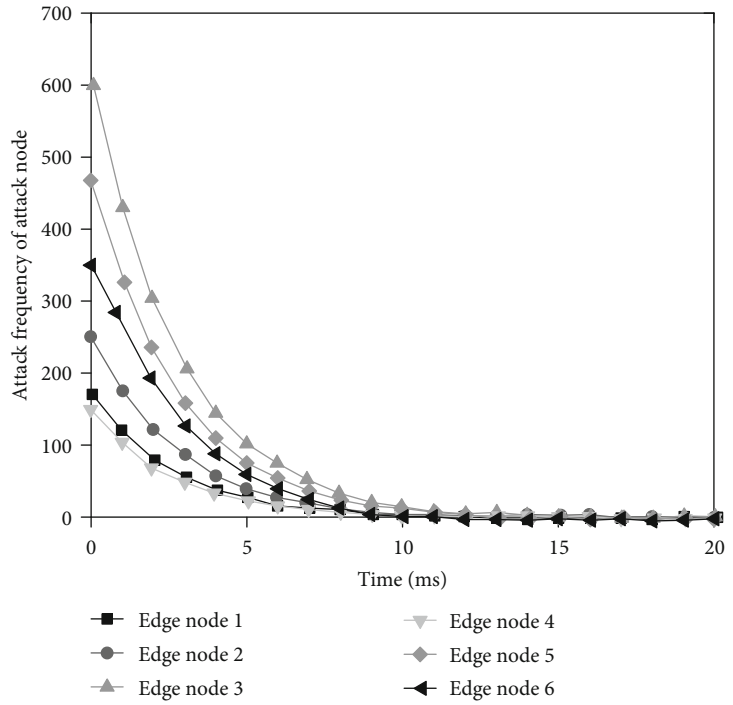

Figure 10: The change of optimal attack frequency of attack node with time.

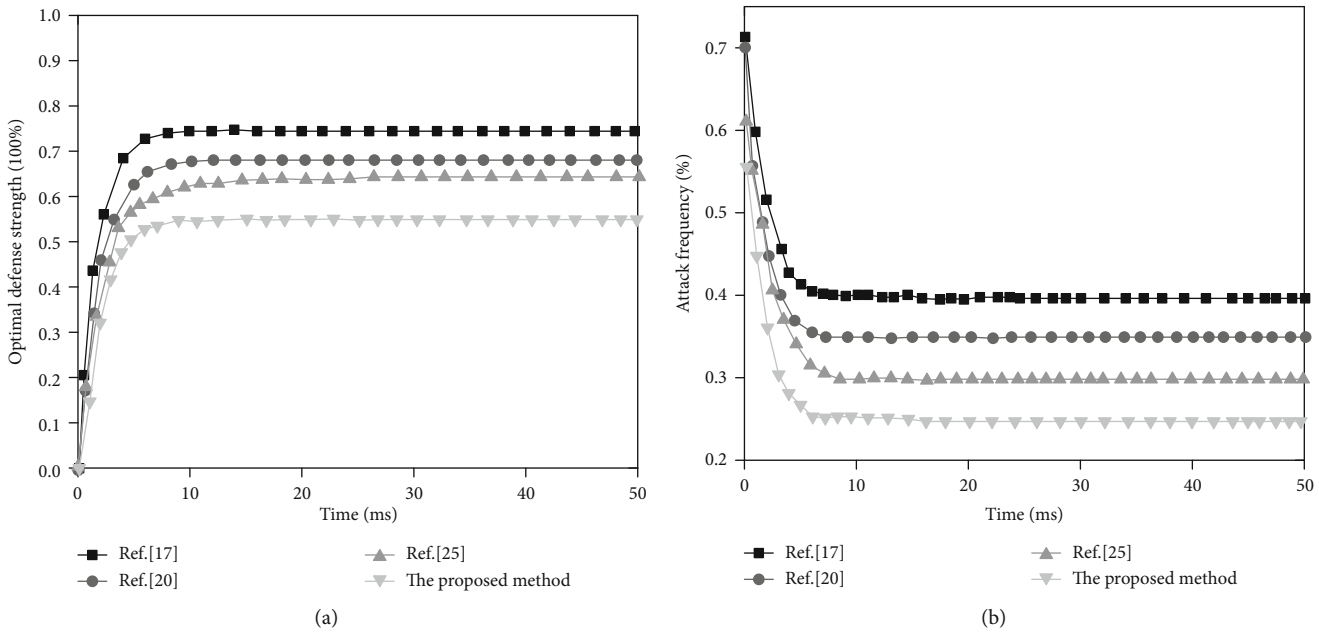

Figure 11: Safety performance comparison of various protection methods.

In order to demonstrate the proposed method security performance, the optimal defense strength and the attack frequency are compared with the defense models proposed in Ref. [17], [20], and [25], as shown in Figure 11.

As Figure 11 shows that with the change of time, the protection methods of the proposed protection method and the comparison method increase rapidly and tend to be stable, while the attack frequency of the intruder is gradually reduced and tends to be stable. However, the proposed method can control the attacker's attack frequency better when the edge intelligent terminal consumes low computing resources.

6. Conclusion

The rapid growth of the number of intelligent terminal devices at the edge of the power distribution IoT leads to the massive physical data generated at the edge of the

network. However, the big data technology based on cloud computing can not meet the low energy consumption and real-time requirements of the edge intelligent terminal for data processing. Edge computing makes up for the deficiency of cloud computing. Edge computing offloads cloud computing services to the network edge. However, the edge network environment is more complex, the heterogeneity between terminal devices and the limited resources of computing and storage make the edge intelligent terminals, and their data face a series of new security challenges. Therefore, a data Security Storage method for power distribution IoT is proposed. Based on the "cloud-tube-edge-end" power distribution IoT structure, a cloud edge collaborative centralized distributed joint control mode is proposed to meet the real-time requirements. The distributed data storage method based on the Kademlia algorithm and encryption algorithm is used to store the data in the ciphertext and execute data query directly on the ciphertext to ensure the security of data storage. In addition, the security protection model of the edge intelligent terminal based on the stochastic differential game is established to ensure the security of the edge intelligent terminal. The results show that the storage and query delay of the proposed method is low, and with the improvement of the storage capacity of the server, the data acquisition delay is less. Moreover, it has better security performance than other methods.

The proposed method assumes that the randomness of the attacker obeys the normal distribution in the process of establishing the model. However, in the actual edge network, the behavior of the attacker is more complex, and the random joining or exiting of the edge intelligent terminal will lead to the change of the edge network structure. Therefore, the edge network based on the randomness of the attacker needs further research. In addition, in order to ensure the data security, the proposed algorithm uses an encryption algorithm and game algorithm at the same time, and the structure is relatively complex. The next research will focus on the design of a data security method which takes into account the security, lightweight, and suitability for the power distribution IoT.

Data Availability

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

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] M. Gusev and S. Dustdar, "Going back to the roots—the evolution of edge computing, an IoT perspective," *IEEE Internet Computing*, vol. 22, no. 2, pp. 5–15, 2018.

[2] Z. Li, M. Shahidehpour, and X. Liu, "Cyber-secure decentralized energy management for IoT-enabled active distribution networks," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 900–917, 2018.

[3] H. Fullmer, "Healthcare power systems may be unprepared for digital age," *Electrical Contractor*, vol. 83, no. 1, pp. 13–13, 2018.

[4] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: deep learning for the internet of things with edge computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, 2018.

[5] R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar, and J. Ott, "Consolidate IoT edge computing with lightweight virtualization," *IEEE Network*, vol. 32, no. 1, pp. 102–111, 2018.

[6] R. Dautov, S. Distefano, D. Bruneo et al., "Metropolitan intelligent surveillance systems for urban areas by harnessing IoT and edge computing paradigms," *Software: Practice and Experience*, vol. 48, no. 8, pp. 1475–1492, 2018.

[7] T. Ogino, S. Kitagami, T. Suganuma, and N. Shiratori, "A multi-agent based flexible IoT edge computing architecture harmonizing its control with cloud computing," *International Journal of Networking and Computing*, vol. 8, no. 2, pp. 218–239, 2018.

[8] F. Ud Din, A. Ahmad, H. Ullah, A. Khan, T. Umer, and S. Wan, "Efficient sizing and placement of distributed generators in cyber-physical power systems," *Journal of Systems Architecture*, vol. 97, pp. 197–207, 2019.

[9] X. Xu, Q. Liu, Y. Luo et al., "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Generation Computer Systems*, vol. 95, no. 6, pp. 522–533, 2019.

[10] C. Pan, M. Xie, and J. Hu, "ENZYME: an energy-efficient transient computing paradigm for ultralow self-powered IoT edge devices," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 11, pp. 2440–2450, 2018.

[11] K. Peng, H. Huang, S. Wan, and V. C. M. Leung, "End-edge-cloud collaborative computation offloading for multiple mobile users in heterogeneous edge-server environment," *Wireless Networks*, vol. 7, no. 4, pp. 2622–2629, 2020.

[12] T. Suganuma, T. Oide, S. Kitagami, K. Sugawara, and N. Shiratori, "Multiagent-based flexible edge computing architecture for IoT," *IEEE Network*, vol. 32, no. 1, pp. 16–23, 2018.

[13] L. Lei, H. Xu, X. Xiong, K. Zheng, W. Xiang, and X. Wang, "Multiuser resource control with deep reinforcement learning in IoT edge computing," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10119–10133, 2019.

[14] T. Ogino, S. Kitagami, and N. Shiratori, "A multi-agent based flexible IoT edge computing architecture and application to ITS," *Journal of Communications*, vol. 14, no. 1, pp. 47–52, 2019.

[15] J. Xue, M. Li, and J. Luo, "Modeling Method for Coupling Relations in Cyber Physical Power Systems Based on Correlation Characteristic Matrix[J]," *Dianli Xitong Zidonghua/Automation of Electric Power Systems*, vol. 42, no. 2, pp. 11–19, 2018.

[16] X. Liu, J. Yu, J. Wang, and Y. Gao, "Resource allocation with edge computing in IoT networks via machine learning," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3415–3426, 2020.

[17] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: from security and efficiency perspectives," *IEEE Network*, vol. 33, no. 2, pp. 50–57, 2019.

[18] Y. Guo, F. Liu, Z. Cai, N. Xiao, and Z. Zhao, "Edge-based efficient search over encrypted data mobile cloud storage," *Sensors*, vol. 18, no. 4, pp. 1189–1203, 2018.

[19] X. Kong, Y. Xu, Z. Jiao, D. Dong, X. Yuan, and S. Li, "Fault location technology for power system based on information about the power Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6682–6692, 2020.

[20] W. Han and Y. Xiao, "Edge computing enabled non-technical loss fraud detection for big data security analytic in Smart Grid," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 4, pp. 1697–1708, 2020.

[21] Z. Lv and H. Song, "Mobile internet of things under data physical fusion technology," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4616–4624, 2020.

[22] Z. Guan, Y. Zhang, G. Si et al., "ECOSECURITY: tackling challenges related to data exchange and security: an edge-computing-enabled secure and efficient data exchange architecture for the energy internet," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 61–65, 2019.

[23] C. A. Pardue, M. L. F. Bellaredj, H. M. Torun, M. Swaminathan, P. Kohl, and A. K. Davis, "RF wireless power transfer using integrated inductor," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 9, no. 5, pp. 913–920, 2019.

[24] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[25] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K.-H. Yeh, "Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing," *Future Generation Computer Systems*, vol. 97, pp. 453–461, 2019.

[26] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[27] S. Kim, K. J. Han, Y. Kim, and S. Kang, "Power integrity coanalysis methodology for multi-domain high-speed memory systems," *IEEE Access*, vol. 7, no. 99, pp. 95305–95313, 2019.

[28] T. Zhuang, M. Ren, X. Gao, M. Dong, W. Huang, and C. Zhang, "Insulation condition monitoring in distribution power grid via IoT-based sensing network," *IEEE Transactions on Power Delivery*, vol. 34, no. 4, pp. 1706–1714, 2019.

[29] C. Fu, C. Peng, X.-Y. Liu, L. T. Yang, J. Yang, and L. Han, "Search engine: the social relationship driving power of Internet of Things," *Future Generation Computer Systems*, vol. 92, pp. 972–986, 2019.

[30] J. Fei and M. Xiaoping, "Fog computing perception mechanism based on throughput rate constraint in intelligent Internet of Things," *Personal and Ubiquitous Computing*, vol. 23, no. 3-4, pp. 563–571, 2019.

[31] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of Things: a comprehensive investigation," *Computer Networks*, vol. 160, no. 9, pp. 165–191, 2019.

[32] M. H. Eldefrawy, N. Pereira, and M. Gidlund, "Key distribution protocol for industrial Internet of Things without implicit certificates," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 906–917, 2018.

[33] Y. Yang, Z. Zheng, K. Bian, L. Song, and Z. Han, "Real-time profiling of fine-grained air quality index distribution using UAV sensing," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 186–198, 2018.

[34] F. Tong, Y. Sun, and S. He, "On positioning performance for the narrow-band internet of things: how participating eNBs impact?," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 423–433, 2019.

[35] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: a review," *Journal of Cleaner Production*, vol. 217, no. 4, pp. 702–715, 2019.

[36] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.

[37] H. Ibrahim, W. Bao, and U. T. Nguyen, "Data rate utility analysis for uplink two-hop internet of things networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3601–3619, 2019.