Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9623934, 10 pages
https://doi.org/10.1155/2022/9623934

Research Article

Microgrid Data Security Sharing Method Based on Blockchain under Internet of Things Architecture

Jian Shang,[1,2] **Runmin Guan**,[2] **and Yuhao Tong**[2]

[1]*Hohai University, College of Computer and Information, Jiangsu, Nanjing 211100, China*
[2]*Jiayuan Technology Co. Ltd., Division of Research and Innovation, Jiangsu, Nanjing 211100, China*

Correspondence should be addressed to Jian Shang; shangjian@jiayuantech.com

Received 18 January 2022; Revised 2 March 2022; Accepted 7 March 2022; Published 4 April 2022

Academic Editor: Shalli Rani

The efficient and secure data sharing mechanism can support the microgrid to achieve more accurate business control, while the current data processing methods have the problems of large computing overhead and low data sharing security. Aiming at the current problems, this paper proposes a microgrid data sharing method based on blockchain technology based on the processing mode of cloud-edge-terminal architecture. Firstly, the elliptic curve encryption algorithm is used on the edge side to encrypt the data collected by the terminal equipment reliably, so as to improve the security and efficiency of microgrid key management. Then, in the cloud, the Reputation-Evaluation Practical Byzantine Fault Tolerant mechanism (REPBFT) based on smart contract and reputation evaluation can effectively manage the data sharing of edge computing devices, avoid the waste of network computing resources, and further improve the efficiency of microgrid data sharing. The simulation results show that when the number of edge devices reaches 25, the calculation and communication overhead of the proposed method are 63.46 ms and 2.66 KB, respectively, and when the processing data reaches 1024 KB, the security of the microgrid system is still 95%, which can realize safe and reliable data sharing and interaction, and can stably support the optimal operation of the microgrid.

1. Introduction

Microgrid aims to promote the consumption of renewable energy and realize multisource power supply for load [1, 2]. Since most distributed generators are closer to the load side, their power supply flexibility and efficiency will be greatly improved, making the power grid operation more efficient and rich [3].

In order to maximize the advantages of renewable energy, the energy interaction between microgrids has developed into a popular method [4]. However, the effectiveness of energy interaction between microgrids largely depends on the authenticity of power generation and consumption information, as well as the efficiency and security of energy transactions [5]. Therefore, it is of great significance to study the efficient and secure data processing between microgrids.

The traditional microgrid adopts centralized operation mode and symmetric encryption algorithm to realize data management and credibility operation, but the data has the risk of being copied and leaked by third-party institutions [6]. In addition, the symmetric encryption algorithm will consume a lot of computing memory in the process of key operation, which is difficult to achieve efficient and reliable data sharing.

The development of blockchain provides a new idea for efficient and reliable interaction of microgrid data [7, 8]. The blockchain generates data into blocks according to the sequence of data time scales and adopts cryptography to ensure that the data cannot be tampered with, so as to realize the security management of massive data [9]. However, it should be pointed out that although the traditional blockchain data processing method can improve the security of data storage to a certain extent, there are few corresponding studies on the efficiency of micro grid data sharing [10], which cannot meet the requirements of safe and efficient data sharing among micro grid groups.

Aiming at the current problems, this paper proposes a microgrid data sharing method based on blockchain based

on the cloud edge collaborative processing mode. The main innovations of the article are as follows:

In order to meet the efficient and fast requirements of microgrid data sharing, this paper uses the elliptic curve encryption algorithm (ECC) to ensure the friendly interaction between microgrid terminal equipment and edge computing devices and improve the security of microgrid data while alleviating the pressure of key management and reducing the system computing overhead.

The collaborative strategy of cloud side interaction is adopted to realize the interoperability and convenience of data sharing between edge computing devices based on cloud smart contract, and Reputation-Evaluation Practical Byzantine Fault Tolerant mechanism (REPBFT) is introduced to complete data information evaluation, which can improve the data processing efficiency of microgrid and ensure the security and credibility of data sharing.

2. Related Research

Microgrid generally consists of distributed power sources such as wind power and photovoltaic, energy storage system, and micropower supply system composed of multicategory loads [11]. Microgrid data has the characteristics of multisource heterogeneity and large quantity. The attribute characteristics of different business data are different, including structured data such as state, electrical, simulation and operation, and semistructured data related to the physical information model [12].

For system controllability, the more reliable the collected data is, the more stable the system operation is [13]. Microgrid system realizes the friendly interaction between source network load and storage through interactive sharing of multidimensional and multi service data and data analysis and fusion based on big data and artificial intelligence algorithms [14]. Therefore, safe and reliable microgrid data sharing is particularly important for users' high-quality power supply and the safe and stable operation of the power grid.

At present, most of the power grid data management adopts the traditional power grid centralized management. Reference [15] proposed a cloud based energy management system to realize microgrid data interaction to realize the optimal operation of low-cost system, but the system may be attacked and lead to data leakage, and the measures only stay at the theoretical level. Reference [16] proposed a privacy protection multiauthority attribute-based smart grid data sharing scheme. The essence of the scheme is centralized computing and processing mode, which has the problem of low encryption efficiency. Therefore, it can be seen that the centralized data sharing interaction mode has been difficult to support the optimal operation of microgrid.

As a popular technology in recent years, blockchain realizes the secure and trusted storage and processing of user data sets by combining database consistency mechanism and cryptography. Reference [17] constructs an encrypted data storage and sharing architecture based on threshold proxy reencryption and blockchain consensus algorithm to meet a wide range of data access requirements. Reference [18] integrates fair data delivery into the phased data delivery protocol in the blockchain consensus process, avoiding third-party data processing and realizing safe data sharing. At the same time, the immutable recording characteristics of blockchain guarantee transactions also provide a new idea for the safe processing of microgrid data [19, 20]. Reference [21] uses blockchain to build a secure and transparent power grid operation allocation model to resist malicious attacks against microgrid; reference [22] realizes continuous monitoring and analysis of materials by integrating audit mechanism and blockchain into the material management and control system of electric power company; reference [23] realizes data analysis of energy management system based on blockchain and reinforcement learning, which can detect improper energy use behavior and improve energy output efficiency; reference [24] reduces the total cost of energy consumption by implementing independent monitoring of intelligent devices and power consumption billing through smart contracts. However, the above reference only analyzes the application security of blockchain in the power grid business scenario, not from the perspective of data sharing security and efficiency trade-off. There is also the problem of uneven distribution of network computing resources, which is difficult to support the stable and reliable operation of microgrid.

To solve this problem, this paper introduces edge computing technology and REPBFT mechanism into the microgrid data security sharing method to support accurate state analysis and fast action execution of the microgrid system.

3. Proposed Method

3.1. Overall Architecture of Microgrid Data Security Sharing. The overall architecture of microgrid data security sharing adopts the data communication mode of cloud side cooperation, as shown in Figure 1. In other words, the edge layer realizes the effective collection of microgrid status data through terminal device registration and data encryption processing. At the same time, the edge layer data information is aggregated and uploaded to the cloud, which shares and accesses data based on smart contracts [25, 26].

3.1.1. Terminal Equipment Layer: Edge Layer. The edge computing device gathers real-time power data collected by terminal equipment such as smart meter, photovoltaic inverter, energy storage converter and wind power inverter. Through the method of "registration before encryption", secure and reliable data transmission between terminal equipment layer and edge layer equipment is realized, the credibility of information interaction between microgrid equipment is guaranteed, and the storage and sharing of multi-dimensional heterogeneous power data are realized.

3.1.2. Edge Layer: Cloud Layer. For the problem of "data island" in the microgrid cloud control center, the cloud–edge-terminal architecture mode and the data sharing and access control model based on smart contract are adopted to realize the stable data sharing between different edge computing devices.

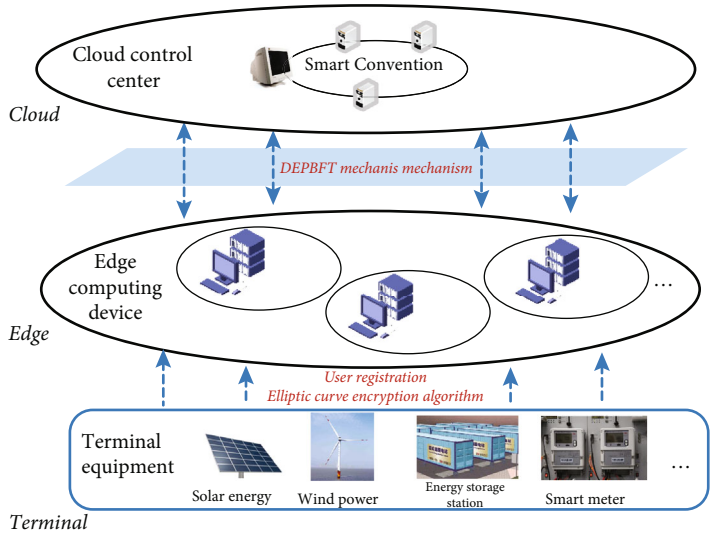

Figure 1: Microgrid data security sharing architecture.

3.2. Terminal Equipment Layer: Edge Layer Equipment Data Acquisition and Encryption. In order to ensure the trusted data interaction between microgrid devices, a trusted terminal device registration mechanism needs to be designed between edge computing devices and terminal devices. The asymmetric encryption algorithm is introduced into the data transmission at both ends to ensure the reliable and safe data collection.

The terminal equipment registration process is as follows:

(1) The terminal device sends the public key and private information of the terminal device, such as physical address and identity information, to the edge computing device

(2) After receiving the terminal device information and checking it, the edge computing device encrypts the public key of the terminal device with the private key of the edge computing device to form a digital signature sign and returns the sign to the terminal device

(3) The terminal device uses its own public key and sign to create an account. Other terminal devices can verify the authenticity of the sign with the public key of the edge computing device, so as to ensure the authenticity of the account

After the terminal equipment completes registration and accesses the edge computing device, it enters the data acquisition stage. At the same time, for security reasons, this paper adds an encryption module for security authentication to the intelligent terminal equipment and edge computing device, realizes the security authentication mechanism through hardware encryption, and encrypts and decrypts the data, as shown in Figure 2.

In the traditional symmetric encryption algorithm, every time a pair of terminal devices use the encryption algorithm, they need to use the unique secret key that other terminals do not know, so that the sending and receiving ends have a large number of keys, resulting in large key management overhead. The asymmetric encryption algorithm represented by elliptic curve encryption algorithm (ECC) uses different secret keys for encryption and decryption. One of the keys is encrypted [27], and the other is used for decryption. Each terminal device only needs to process a pair of keys, so as to reduce the corresponding key management burden and reduce the system computing overhead. The flow chart of asymmetric encryption algorithm is shown in Figure 3.

In this paper, the ECC encryption algorithm is used to realize data trusted processing. The encryption process is as follows:

(1) Determine the finite field F_p, which has and has only p elements

(2) Terminal equipment a selects elliptic curve $E_p(a, b)$ in the finite field and takes a point on the elliptic curve as the base point D

(3) The terminal device a randomly selects a prime number between $1 \sim p - 1$ as the private key k and generates the public key $K = kD$ according to the addition rule

(4) Terminal equipment a transmits $E_p(a, b)$ and points K and D to terminal equipment B

(5) After receiving the information, terminal equipment B encodes the plaintext to be transmitted to a point H on $E_p(a, b)$ and generates a random integer e $(0 < e < 1)$

(6) Terminal equipment B calculation points $C_1 = H + eK$, $C_2 = eD$

(7) Terminal equipment B transmits C_1 and C_2 to terminal equipment A

(8) After receiving the information, terminal device A calculates $C_1 \sim kC_2$, determines point H, and then decodes point H to obtain plaintext

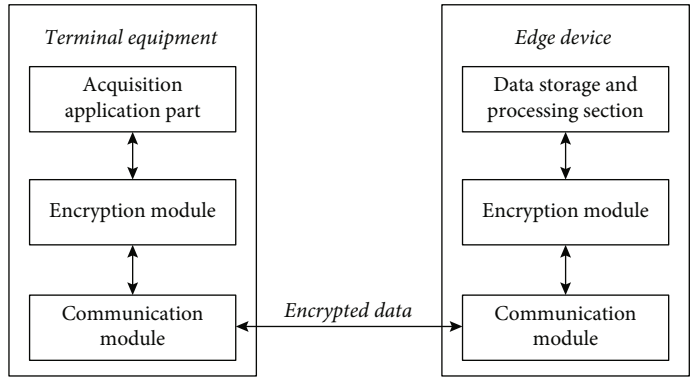

Figure 2: Encrypted communication mode between terminal equipment and edge computing device.

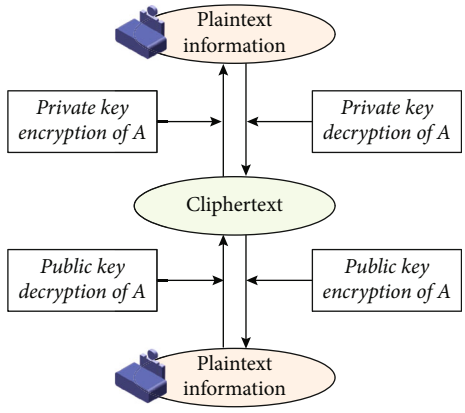

Figure 3: Asymmetric encryption algorithm flow.

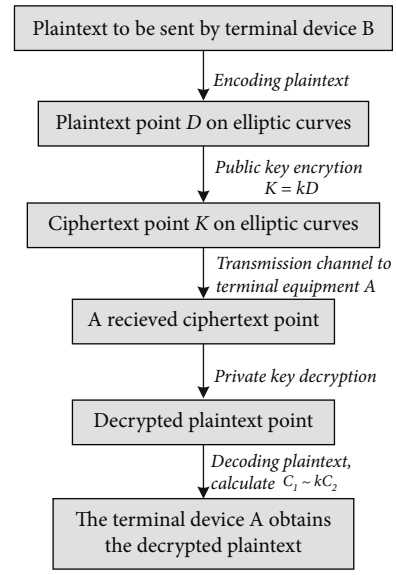

Figure 4: ECC encryption process.

In this process, the attacker can only obtain $E_p(a, b)$, K, D, C_1, and C_2. It is very difficult to obtain k through K and D or e through C_2 and D. It is difficult to steal the plaintext transmitted between terminal devices.

Figure 4 shows the encryption and decryption flow of the elliptic curve algorithm.

3.3. Data Security Sharing. It can be seen from the above analysis that the data of each downstream terminal device is stored in the microgrid edge computing device. Further, based on blockchain, this paper realizes the secure data sharing of microgrid in the mode of cloud-edge-terminal architecture.

Based on the cloud-edge-terminal architecture, the proposed data security sharing scheme links the adjacent edge computing devices into a private chain to realize the data sharing of terminal devices. The method includes the following entities: edge computing devices, terminal devices, private chains, and smart contracts for cloud control centers. As shown in Figure 5, the data security sharing scheme is divided into two modules according to functions. The left is the data sharing model, and the right is the blockchain. The data sharing model supports the storage of the blockchain, and the blockchain supports the security protection of the data sharing model. The microgrid user transmits the storage request to the edge computing device through the terminal device, and the process is recorded in the blockchain.

In this paper, offchain storage is used, only the user name, user address, and recorded information are stored in the block, the collected original microgrid data is stored in the storage node of the edge computing device, and the ECC algorithm described above is used to encrypt the data.

The steps of data sharing are as follows:

(1) Register edge computing devices and terminal devices, and the system does not allow unregistered edge computing devices and terminal devices to join data sharing

(2) The registered terminal device initiates a data storage request to the edge computing device and uploads its own data to the edge computing device through the encryption mechanism proposed above

(3) The edge computing device 1 publishes the data to the smart contract through the private chain on

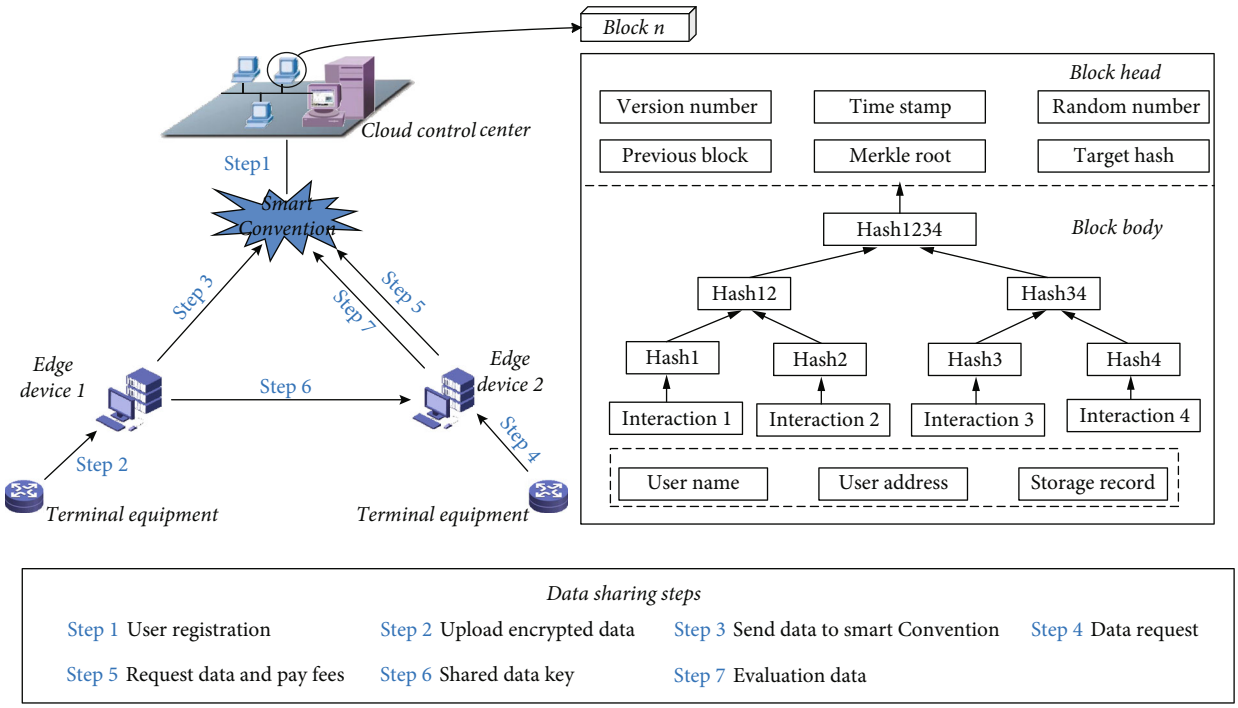

Figure 5: Model diagram of data sharing system.

behalf of the terminal device, so that the terminal device can request and retrieve the data information

(4) If the terminal equipment downstream of the edge computing device 2 requires shared data, it is necessary to initiate a request for shared data

(5) The edge computing device 2 requests the key of encrypted data from the smart contract on behalf of the terminal device

(6) The edge computing device 1 sends the key of the encrypted data to the edge computing device 2, so that the edge computing device 2 obtains the permission to access the data, and encrypts and transmits the data to its downstream terminal device

(7) The terminal equipment will evaluate the shared data, and the system will also check the evaluation to prevent abnormal evaluation

3.3.1. Consensus Mechanism for Block Generation. This paper uses the consensus mechanism based on REPBFT to evaluate the trusted data sharing process between edge computing devices. The credit evaluation algorithm in REPBFT is mainly composed of reward mechanism and punishment mechanism. The credit value is mainly used as a reference for preferentially responding to the request of the edge computing device. The rewards include the following: actively initiating change messages, reporting and sending false information, and contributing idle computing power.; Penalties include the following: sending false messages and falsely accusing other edge computing devices, as shown under the credit evaluation algorithm.

Among them, w_1, w_2, and w_3 are the parameters of reward mechanism, and v is the parameters of punishment mechanism. The calculation formula is as follows:

$$w_1(T, L, O) = \alpha \frac{O_i}{e^{L_{ij}} T^2}, \tag{1}$$

$$w_2(T, L, O) = \alpha \frac{O_i}{e^{L_{ij}} F^2}, \tag{2}$$

$$w_3(L, O_i, N_i) = \alpha \frac{N_i}{e^{L_{ij}} O_i}, \tag{3}$$

$$v(F, L, O_i) = -\beta \frac{O_i}{e^{L_{ij}} F^2}, \tag{4}$$

where α is the system reward coefficient, β is the system penalty coefficient, T is the real message level, and F is the level of false information. When V_i sends the data information M_{V_i} to the system, V_i can first obtain the reward for actively providing idle computing power last time, that is, the current credit value plus $w_3(L, O_i, N_i)$, and then N starts counting again from 0. If no device reports V_i, the credit value of V_i can be added with $w_1(T, L, O)$. In addition, when a device reports V_i data information, the cloud control center judges the report. If the report is true, the credit value of the device initiating the report can increase $w_2(T, L, O)$, and the V_i sending false information will be punished.

3.3.2. Data Sharing Method. On the basis of trusted data processing between edge computing devices, cloud control center is further introduced to realize trusted data sharing. When the terminal device requests data, it will notify the proxy edge computing device, and the proxy edge

Input M_{V_i} is the data information transmitted by the edge computing device i; M_{ij} is the edge computing device V_i reporting data information to V_j; L_{ij} is the distance between edge computing device V_i and V_j; O is the data density of cloud control center; N_i is the number of times the edge computing device provides idle computing power;
Output Re_{V_i} ⊠Re_{V_j}
1) if M_{ij} does not exist
2) for V_i perform $\mathrm{Re}_{V_i} \longleftarrow \mathrm{Re}_{V_i} + w_1(T_{M_{V_i}}, L_{ij}, O_i) + w_3(L_{ij}, O_i, N_i)$
3) end for
4) else
5) if M_{V_i} is ture
6) for V_i perform $\mathrm{Re}_{V_i} \longleftarrow \mathrm{Re}_{V_i} + w_1(T_{M_{V_i}}, L_{ij}, O_i) + w_3(L_{ij}, O_i, N_i)$
7) end for
8) end if
9) end if

Algorithm 1: Reputation Evaluation Algorithm ().

computing device will initiate a data request to the cloud control center.

(1) requestKey() generates a transaction Y according to the parameters input by the terminal device, where $\mathrm{EA}_{\mathrm{Rdevice}}$ is the private chain address when the terminal device requests data; $\mathrm{EA}_{\mathrm{REdge}}$ is the address when the edge computing device requests data; $\mathrm{EA}_{\mathrm{SEdge}}$ is the address when the edge computing device returns data; $\mathrm{ID}_{\mathrm{data}}$ is the data identification of the purchase. t is the time when the edge computing device initiates the purchase request, and S is the unique identification of a transaction

$$Y = \left(ID_Y, \mathrm{EA}_{\mathrm{Rdevice}}, \mathrm{EA}_{\mathrm{REdge}}, \mathrm{EA}_{\mathrm{SEdge}}, \mathrm{ID}_{\mathrm{data}}, t\right), \quad (5)$$

$$\mathrm{ID}_Y = \left(\mathrm{EA}_{\mathrm{Rdevice}}, \mathrm{EA}_{\mathrm{buyer}}, \mathrm{EA}_{\mathrm{seller}}, \mathrm{ID}_{\mathrm{data}}, t\right). \quad (6)$$

(2) The edge computing device 1 digitally signs the transaction $\mathrm{Sign}(Y, v_{\mathrm{REdge}})$ using its elliptic curve private key and sends the public key v_{REdge}, signature message Sign and requests plaintext Y of the edge computing device to the cloud control center

(3) The edge computing device 2 verifies the signature $(Y, \mathrm{Sign}, v_{\mathrm{REdge}})$ of the edge computing device 1 with the transaction Y, the signature message Sign, and the public key v_{REdge} to confirm that there is no problem with the identity of the edge computing device 1

(4) The edge computing device 2 encrypts the key cv of the encrypted data $W_{\mathrm{cv}}(\mathrm{data})$ with the public key v_{REdge} of the edge computing device 1 by the elliptic curve encryption algorithm, and the ciphertext obtained by the elliptic curve encryption algorithm is $\mathrm{CT}(v_{\mathrm{REdge}}, \mathrm{cv})$

(5) The edge computing device 2 transmits the ciphertext CT to the edge computing device 1 through the cloud control center

In order to ensure the credibility of the data provided by the edge computing device, the terminal equipment needs to evaluate the data after obtaining the data, which will affect the credit value of the edge computing device.

σ is defined as the number of evaluations, σ_{bad} is the number of poor evaluations, $\sigma = \sigma_{\mathrm{good}} + \sigma_{\mathrm{bad}}$, and Z_{PEdge} is the credit value of the edge computing device 1.

The calculation formula is as follows:

$$Z_{\mathrm{PEdge}} = \begin{cases} Z_{\mathrm{PEdge}} & 0 \le \sigma_{\mathrm{bad}} \le \dfrac{1}{5}\sigma, \\ Z_{\mathrm{PEdge}} - \lambda \cdot \dfrac{\sigma_{\mathrm{bad}}}{\sigma} & \dfrac{1}{5}\sigma \le \sigma_{\mathrm{bad}} \le \dfrac{4}{5}\sigma, \\ Z_{\mathrm{PEdge}} - \gamma^{\frac{\sigma_{\mathrm{bad}}}{\sigma}} & \dfrac{4}{5}\sigma \le \sigma_{\mathrm{bad}} < \sigma, \end{cases} \quad (7)$$

where λ and γ are regulatory factors, $\lambda > 1$, $\gamma > 1$.

According to formula (7), when the number of negative comments is less than $\sigma/5$, the credit value of the edge computing device will not decrease. When the number of bad comments is in the interval $[\sigma/5, 4\sigma/5]$, it indicates that the data quality provided by the edge computing device needs to be improved, and the credit value will be reduced. When the number of negative comments is in the range $[4\sigma/5, \sigma]$, it indicates that the data provided by the edge computing device has a large problem, and the credit value will be greatly reduced.

In order to prevent the abnormal evaluation of the terminal equipment from affecting the credit value of the edge computing device, an evaluation check mechanism is used to restrict the evaluation behavior of the terminal equipment.

(1) Determination of Untrusted terminal Equipment. It is assumed that in a cycle time, an edge computing device receives σ evaluations from i terminal devices, the total

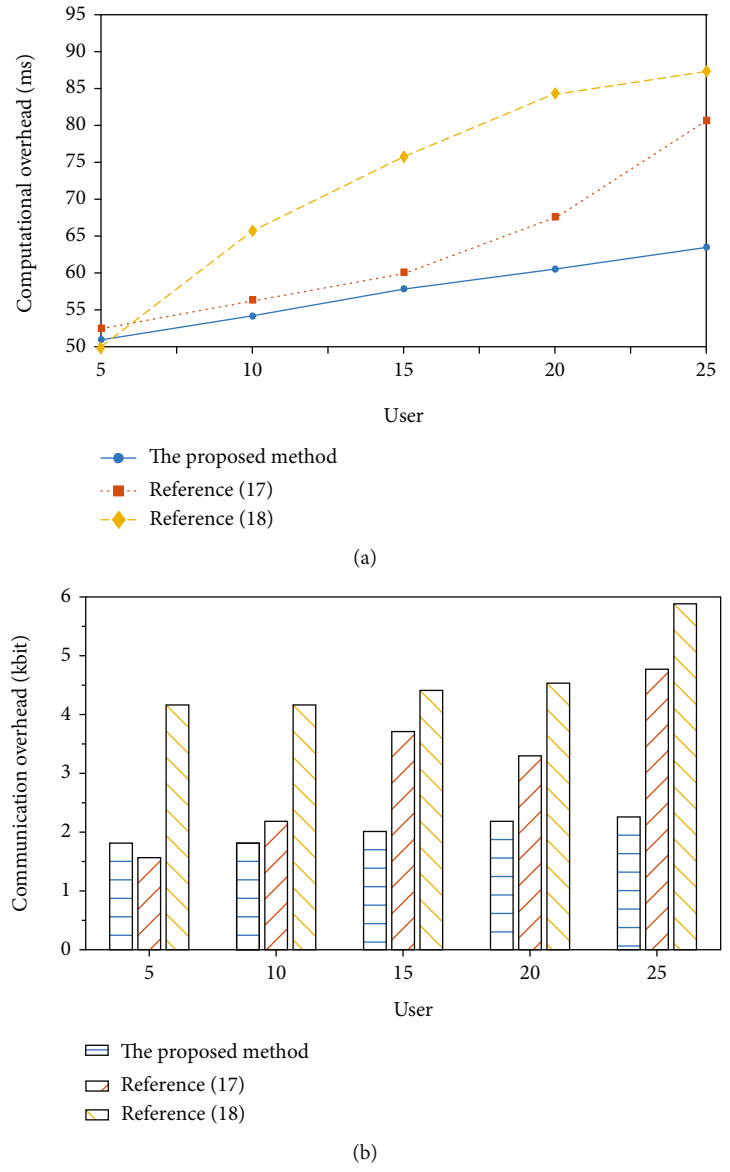

Figure 6: Algorithm performance under different methods.

number of terminal devices $i = i_{good} + i_{bad}$, and the total number of terminal devices $\sigma = \sigma_{good} + \sigma_{bad}$.

$\max(\sigma_{good}, \sigma_{bad})$ is used to represent the evaluation results of most terminal equipment. If the vast majority of terminal devices are high praise $\sigma_{good} = \max(\sigma_{good}, \sigma_{bad})$, the i_{good} terminal devices with high praise are honest terminal devices, while the i_{bad} terminal devices with poor evaluation are untrusted terminal devices. On the contrary, the same is true.

(2) Judgment of Abnormal Terminal Equipment. Count the determination times of untrusted terminal equipment in a certain period. If the number of times the terminal equipment is determined to be untrusted exceeds the threshold, it is determined that the terminal equipment is an abnormal terminal equipment.

4. Experiment and Analysis

The experimental environment uses 30 hosts to build the proposed microgrid data sharing system, of which 5 are used as edge computing devices, the hardware is set as 32 GB memory and Intel i5 processor, the remaining 25 are used as terminal devices, and the hardware is set as 16 GB memory and Intel I3 processor. The data storage nodes in the blockchain are interconnected by distributed architecture between hosts.

In the experiment, relying on the Ubuntu 20.04 operating system realizes software operation. Remix IDE (2020.6.4 last version) is used as the development tool of private chain smart contract, the program is written in Solidity language, and the private chain adopts MetaMask software.

4.1. Algorithm Overhead Analysis. In order to better support the edge computing device to realize data trusted

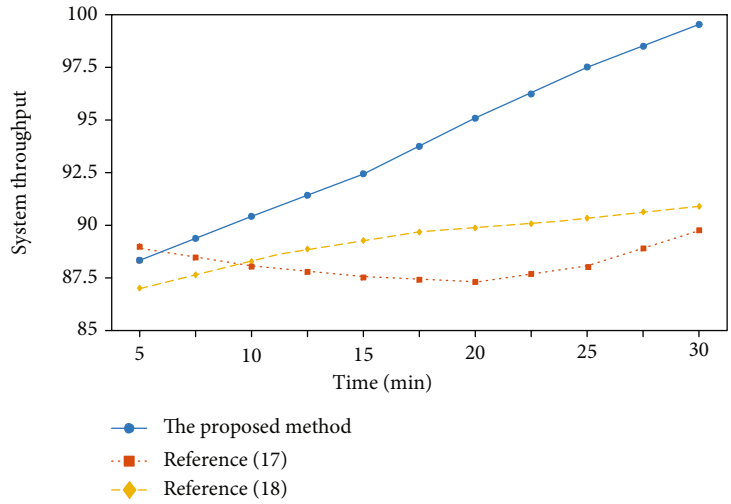

Figure 7: System throughput under different methods.

transmission, this paper uses different encryption methods for comparative analysis. This paper realizes the simulation experiment analysis based on charm library. Charm library is a function library that can be used for prototype development of the cryptosystem. This paper selects secp384r1 elliptic curve from charm library to test the system performance. At the same time, reference [17] and reference [18] are used as comparison methods to prove the optimality of algorithm overhead performance. In the same operating environment, the least algorithm overhead proves that it can better support the microgrid and realize the optimal data interaction.

Figure 6 shows the calculation and communication overhead under three methods.

As shown in Figure 6, the calculation and communication overhead under the three data processing methods increase linearly with the increase of the number of terminal equipment access. When $n = 25$, the data analysis performance of the proposed method is the best. The calculation and communication overhead of microgrid data encryption are 63.46 ms and 2.36 KB, respectively. The network performance under the comparison method is poor. The calculation and communication overhead in reference [18] are 87.32 ms and 5.87 KB, respectively. At the same time, the calculation overhead curve in reference [17] changes in the form of quasiexponential. There is a risk of system downtime when the number of users is large. This is because the introduction of ECC algorithm not only reduces the calculation consumption of key management but also effectively releases the corresponding algorithm efficiency and improves the communication performance to a certain extent. In contrast, although the comparison method releases the processing pressure of the third party to a certain extent, it still has some limitations in computing power and communication memory.

The essence of network throughput is the total amount of data passing through the network in unit time, which can evaluate the operation of the network. Therefore, this paper further carries out optimization analysis based on the network throughput index in literature [17] and literature [18], as shown in Figure 7.

As can be seen from Figure 7, with the increase of time, both the proposed method and the microgrid under reference [18] obtain higher system throughput, while the system throughput in reference [17] decreases first and then increases and remains relatively stable in the range (87, 90). The system throughput reaches the minimum value at 20 min. However, the throughput of reference [18] and the method in this paper change with time and have good network sensitivity. In contrast, the change of system throughput in this paper is faster than that in reference [18], which can realize the linear change of higher proportion coefficient in the simulation run cycle. Therefore, it can be proved that the incentive mechanism added in the proposed method is effective. The reward mechanism will reward the profit of the edge computing devices that contribute resources, and the punishment mechanism will punish the abnormal nodes, which ensures that the edge computing devices can actively participate in the consensus process, reduces the probability of abnormal nodes participating in the consistency, and effectively improves the throughput of the system. The consensus mechanism in the comparison method does not involve the analysis and discussion of the corresponding reward and punishment coefficient. Therefore, in this experiment, it is realized that the performance of the comparison method is far worse than that of the proposed method.

4.2. Safety Analysis. The proposed data sharing method adopts a series of means such as ECC algorithm, REPBFT mechanism, and smart contract to improve the credibility and security of data. Therefore, the proportion of abnormal data sharing behaviors such as resisting external attacks is taken as the security analysis standard, and the specific index is the ratio of the number of successful prevention of abnormal data sharing to the number of all abnormal data sharing.

In this paper, reference [22] and reference [23] are used as comparative methods for optimal comparative analysis of

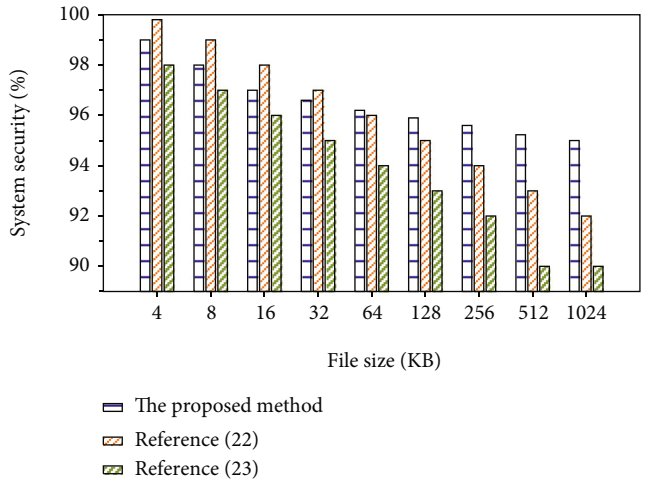

Figure 8: Comparison of safety performance of different methods.

security. All data processing methods are implemented in the same experimental environment. The security comparison of different methods is shown in Figure 8.

The larger the file, the more data to be shared, and better data sharing and interaction can be achieved.

As can be seen from Figure 8, compared with other comparison methods, the proposed method has the highest security performance and can resist the most external network threats. When the file size reaches 1024 KB, its security is 95%, much higher than 80%. In reference [23], when the file size is 512 KB, the security has been reduced to about 90%.

The reason is that ECC algorithm and REPBFT mechanism are introduced into the data sharing method to realize efficient and reliable data encryption and friendly interaction between devices, so as to avoid invalid data occupying limited resources. At the same time, relying on the cloud-edge-terminal architecture model, the data sharing and access control model based on smart contract realizes the friendly interaction and stable sharing of data between different edge computing devices. However, there is a lack of analysis and discussion on the status of network nodes in the comparative reference, which leads to the waste of network resources to a certain extent and reduces the data flow efficiency of microgrid.

5. Conclusion

In order to realize the secure and trusted sharing of microgrid data, this paper proposes a data sharing method based on cloud-edge-terminal architecture mode and blockchain. After the terminal device registration step, the trusted data encryption between the terminal device and the edge computing device is realized by using the elliptic encryption algorithm. The REPBFT mechanism is introduced into the cloud-edge-terminal architecture to realize the effective utilization of microgrid network computing resources, reduce the system computing overhead, and improve the security of data sharing. Experimental results show that the proposed method can meet the security and efficiency requirements of microgrid data sharing.

With the continuous promotion of energy Internet strategy, power grid data also presents an explosive growth form. This paper still lacks in-depth consideration on the refinement of computing capacity of data sharing model. In the next research, we need to consider the mode capacity of shared storage and the scalability of blockchain to meet the rapidly growing demand for power data processing.

Data Availability

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Li and W. Qi, "Toward optimal operation of internet data center microgrid," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 971–979, 2018.

[2] K. Moharm, "State of the art in big data applications in microgrid: A review," *Advanced Engineering Informatics*, vol. 42, no. 1, pp. 100913–100945, 2019.

[3] J. Arkhangelski, A. T. Mahamadou, and G. Lefebvre, "Day-ahead optimal power flow for efficient energy management of urban microgrid," *IEEE Transactions on Industry Applications*, vol. 57, no. 2, pp. 1285–1293, 2021.

[4] O. Ciftci, M. Mehrtash, and A. K. Marvasti, "Data-driven nonparametric chance-constrained optimization for microgrid energy management," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2447–2457, 2020.

[5] H. M. Huang, F. Liu, X. M. Zha et al., "Robust bad data detection method for microgrid using improved ELM and DBSCAN algorithm," *Journal of Energy Engineering*, vol. 144, no. 3, p. 04018026, 2018.

[6] S. Pouraltafi-kheljan, M. Ugur, E. Bozulu, B. C. Çalişkan, O. Keysan, and M. Gol, "Centralized microgrid control system in compliance with IEEE 2030.7 standard based on an advanced field unit," *Energies*, vol. 14, no. 21, pp. 1–31, 2021.

[7] B. Liu, M. Wang, J. Men, and D. Yang, "Microgrid trading game model based on blockchain technology and optimized particle swarm algorithm," *Access*, vol. 8, no. 1, pp. 225602–225612, 2020.

[8] W. T. Zhao, J. Lv, X. L. Yao et al., "Consortium Blockchain-based microgrid market transaction research," *Energies*, vol. 12, no. 20, pp. 3812–3822, 2019.

[9] B. Kirpes, E. Mengelkamp, G. Schaal, and C. Weinhardt, "Design of a microgrid local energy market on a blockchain-based information system," *IT - Information Technology*, vol. 61, no. 2-3, pp. 87–99, 2019.

[10] J. Kim, Y. Chang, and D. H. Choi, "Intelligent micro energy grid in 5G era: platforms, business cases, testbeds, and next generation applications," *Electronics*, vol. 8, no. 4, pp. 422–468, 2019.

[11] H. Qiu, W. Gu, X. Xu et al., "A historical-correlation-driven robust optimization approach for microgrid dispatch," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1135–1148, 2021.

[12] D. S. De and R. Prasad, "Digitalization of global cities and the smart grid," *Wireless Personal Communications*, vol. 113, no. 3, pp. 1385–1395, 2020.

[13] A. Hussain, A. O. Rousis, I. Konstantelos, G. Strbac, J. Jeon, and H. M. Kim, "Impact of uncertainties on resilient operation of microgrids: a data-driven approach," *IEEE Access*, vol. 7, no. 1, pp. 14924–14937, 2019.

[14] L. Cheng, Y. Jia, and X. Zhao, "DRO-MPC-based data-driven approach to real-time economic dispatch for islanded microgrids," *IET Generation Transmission & Distribution*, vol. 14, no. 24, pp. 5704–5711, 2020.

[15] E. Anthi, A. Javed, O. Rana, and G. Theodorakopoulos, "Secure data sharing and analysis cloud-based energy management systems," in *Proceedings of cloud infrastructures, services, and IoT Systems for Smart Cities*, pp. 228–242, Springer, Cham, 2018.

[16] L. Zhang, J. Ren, Y. Mu, and B. Wang, "Privacy-preserving multi-authority attribute-based data sharing framework for smart grid," *IEEE Access*, vol. 8, no. 1, pp. 23294–23307, 2020.

[17] Y. W. Chen, B. W. Hu, H. J. Yu, Z. Duan, and J. Huang, "A threshold proxy re-encryption scheme for secure IoT data sharing based on blockchain," *Electronics*, vol. 10, no. 19, pp. 1–18, 2022.

[18] L. Wang, J. Y. Liu, and W. Y. Liu, "Staged data delivery protocol: a blockchain-based two-stage protocol for non-repudiation data delivery," *Concurrency and Computation-Practice & Experience*, vol. 33, no. 13, pp. 1–20, 2021.

[19] L. Wang, J. Wu, R. Yuan et al., "Dynamic adaptive cross-chain trading mode for multi-microgrid joint operation," *Sensors*, vol. 20, no. 21, pp. 6020–6096, 2020.

[20] Z. L. Zhao, J. T. Guo, X. Luo et al., "Energy transaction for multi-microgrids and internal microgrid based on blockchain," *IEEE Access*, vol. 8, no. 1, pp. 144362–144372, 2020.

[21] W. Xu, J. Li, M. Dehghani, and M. GhasemiGarpachi, "Blockchain-based secure energy policy and management of renewable-based smart microgrids," *Sustainable Cities and Society*, vol. 72, no. 6, p. 103010, 2021.

[22] A. Marín-López, S. Chica-Manjarrez, D. Arroyo, F. Almenares-Mendoza, and D. Díaz-Sánchez, "Security information sharing in smart grids: persisting security audits to the blockchain," *Electronics*, vol. 9, no. 11, pp. 1816–1865, 2020.

[23] G. Vasukidevi and T. Sethukarasi, "BBSSE: blockchain-based safe storage, secure sharing and energy scheme for smart grid network," *Wireless Personal Communications*, vol. 4, no. 1, pp. 1–22, 2021.

[24] M. Afzal, Q. Huang, W. Amin, K. Umer, A. Raza, and M. Naeem, "Blockchain enabled distributed demand side management in community energy system with smart homes," *IEEE Access*, vol. 8, no. 1, pp. 37428–37439, 2020.

[25] S. S. Karthik and A. Kavithamani, "Fog computing-based deep learning model for optimization of microgrid-connected WSN with load balancing," *Wireless Networks*, vol. 27, no. 4, pp. 2719–2727, 2021.

[26] Q. L. Duan, N. V. Quynh, H. M. Abdullah et al., "Optimal scheduling and management of a smart city within the safe framework," *IEEE Access*, vol. 8, no. 1, pp. 161847–161861, 2020.

[27] K. Aldriwish, "A double-blockchain architecture for secure storage and transaction on the Internet of Things networks," *International Journal of Computer Science and Network Security*, vol. 21, no. 6, pp. 119–126, 2021.