Hindawi
Journal of Electrical and Computer Engineering
Volume 2023, Article ID 9861845, 1 page
https://doi.org/10.1155/2023/9861845

Retraction

Retracted: A Microgrid Security Defense Method Based on Cooperation in an Edge-Computing Environment

Journal of Electrical and Computer Engineering

Received 19 December 2023; Accepted 19 December 2023; Published 20 December 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Shang, R. Guan, and C. Shen, "A Microgrid Security Defense Method Based on Cooperation in an Edge-Computing Environment," *Journal of Electrical and Computer Engineering*, vol. 2023, Article ID 1856876, 9 pages, 2023.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2023, Article ID 1856876, 9 pages
https://doi.org/10.1155/2023/1856876

Research Article

A Microgrid Security Defense Method Based on Cooperation in an Edge-Computing Environment

Jian Shang,[1,2] **Runmin Guan**,[2] **and Changlu Shen**[2]

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

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

Received 4 June 2022; Revised 21 July 2022; Accepted 25 July 2022; Published 5 May 2023

Academic Editor: Xuefeng Shao

Aiming at the problems of high delay and vulnerable to network attack in the traditional microgrid centralized architecture, a collaborative microgrid security defense method in the edge-computing environment is proposed. First, we build the edge-computing framework for microgrid, deploy the edge-computing server near the equipment terminal to improve the data processing efficiency, and deploy the blockchain in the edge server to ensure the reliability of the system. Then, the fully homomorphic encryption algorithm is used to design the smart contract, and the secure sharing of information is ensured through identity authentication, data encryption call, and so on. Finally, the credibility model is integrated into the election algorithm and is used to build a trusted edge cooperation mechanism to further improve the ability of the system to defend against network attacks. Based on the microgrid model, the experimental demonstration of the proposed method is carried out. The results show that when subjected to a network attack, the current fluctuation range is small and the defense success rate exceeds 95%, which is better than other methods and can better meet the requirements of practical application.

1. Introduction

With the rapid development of network technology and the wide application of advanced sensing equipment, the microgrid system has become more intelligent, large scale, and information-based [1]. The cloud computing model can centrally manage large-scale data and flexibly manage computing, which can meet the medium- and long-term needs of microgrid big-data computing, but the effect of time-sensitive real-time business processing is not ideal [2, 3]. Therefore, how to efficiently process microgrid data has become an urgent problem to be solved.

At the same time, the high integration of microgrid and information and communication technology makes it have a large number of security vulnerabilities, especially the update and upgrading of network attack technology has brought new problems to information security [4]. In the recent years, the maturity of computer network technology also makes the way of network attacks more and more hidden and destructive. The microgrid mostly adopts the distributed operation mode, so the threat of network attack becomes more and more serious, which not only has a bad impact on the safe and stable operation of the microgrid but also the incidence of power grid accidents caused by a network attack is increasing year by year [5]. Therefore, the research on microgrid security defense is of great significance.

For the security defense scheme of distributed microgrids, there have been many research results at home and abroad. For example, Obert and Chavez [6] proposed a method using lightweight anomaly detection and the graph theory to effectively monitor and classify potential threats in the smart grid. However, the processing ability of massive microgrid data needs to be improved. Zhang and Zhao [7] proposed a smart grid data security protection management platform, which effectively ensures the network data security of all links of power grid transmission, transformation, and distribution from the aspects of data label and authority setting. The platform focuses on the data protection of the whole process of transmission, transformation, and

distribution, which is not obvious for the data characteristics of the microgrid. Suo and Zhou [8] proposed a computer-aided analysis system of relay protection based on data mining. The data mining technology is applied to the relay protection fault information processing system, and the data mining technology is used to extract many potentially important factors, facts, and correlations contained in a large number of fault information. However, the efficiency of data mining is low, which is not conducive to the real-time protection of the microgrid. Hasan et al. [9] strictly review the blockchain implementation of network security perception and energy data protection in the smart grid. On the basis of discussing the security problems of the smart grid system, blockchain technology is applied to solve the main security problems of smart grid scenario. However, the background environment of edge calculation is not considered, and the calculation mode is slightly different. Oksuz [10] proposed an efficient data aggregation and dynamic billing system, which uses anonymous communication to exchange information between smart meters and the cloud, combined with blockchain technology to aggregate user data integrity and protect user data privacy. Zhong and Xiong [11] designed a data security protection method for distribution network based on homomorphic encryption and the secret-sharing algorithm, established the edge node security protection model based on noncooperative differential games, and designed the edge node optimal defense strategy algorithm. However, the addition of data security protection leads to high communication delays, and the overall efficiency of the system needs to be further improved.

Based on the abovementioned analysis, aiming at the problems of data delay and vulnerability to network attacks that exist widely in most of the existing security defense methods, a collaborative microgrid security defense method in the edge-computing environment is proposed. Edge computing is introduced to localize data and reduce data transmission delay. At the same time, blockchain technology is used to design a network security model and improve the ability of the system to resist network attacks through the optimization of smart contracts. Compared with the traditional centralized cloud computing architecture, the innovation of the proposed method lies in the following:

(1) The edge-computing architecture is introduced to realize the nearby deployment of computing nodes, so as to build a microgrid model based on edge cooperation. Through the localization analysis and control of data, the management efficiency of distributed devices is improved.

(2) The security defense of the edge network is realized based on the blockchain technology, in which the homomorphic encryption algorithm is introduced to design the smart contract, and the credibility model is integrated into the election algorithm to build a credible edge cooperation mechanism, so as to comprehensively improve the security of the microgrid.

2. Microgrid Security Model in an Edge Computing Environment

2.1. Microgrid Architecture Based on Edge Computing. In the traditional microgrid centralized-cloud computing model, the data transmission loop between the device and the cloud is long, and the real-time data processing is insufficient. Therefore, the edge-computing model is introduced to deploy corresponding servers near the network edge of the terminal device for localized data statistical analysis. There is no need to transfer all data to the cloud center to further shorten the time of data analysis and reduce the data congestion of the cloud platform [12]. Microgrid architecture based on edge computing is shown in Figure 1.

The equipment layer is composed of all equipment in the microgrid, such as transformer and other conversion device and controlled load. The edge layer includes edge gateway, edge platform, and edge service. It provides computing and other services at the network edge close to the device layer. The cloud layer provides various cloud computing services, and the corresponding cloud center type can be selected according to the different microgrid scales.

Among them, the edge gateway is generally deployed near the power generation equipment, power conversion device, energy storage device, and unstable load with large fluctuation. The real-time data of equipment in the area are transmitted to the same edge gateway, and the data are exchanged through the network port and uploaded to the edge platform at the same time [13]. The edge platform is operated synchronously by various edge gateways distributed in the system. It runs in an open-source environment and can provide various management business applications and microservices for microgrid [14]. The platform not only collects the real-time device data of the storage edge gateway but also sends it to the cloud center after preprocessing and accepts the corresponding control. Edge services cooperate between edge resources and cloud center resources and edge resources through edge cloud cooperation and edge cooperation, so as to maximize the computing and storage capacity of edge-computing architecture.

2.2. Microgrid Security Model Based on Blockchain Technology. The edge-computing architecture for microgrid aims to reduce the pressure of cloud center servers in the system through edge computing, but the edge environment far away from the central control is more vulnerable to network attacks. Therefore, the blockchain network is used to organize each edge-computing server node to form an edge side network to improve the security of the microgrid. The distributed ledger of blockchain provides a more transparent and controllable data privacy protection mechanism [15]. Deploying the edge-computing architecture and the blockchain on the edge server at the same time can not only ensure that the blockchain can use the microgrid computing resources but also ensure that the edge computing can process the microgrid data in a trusted

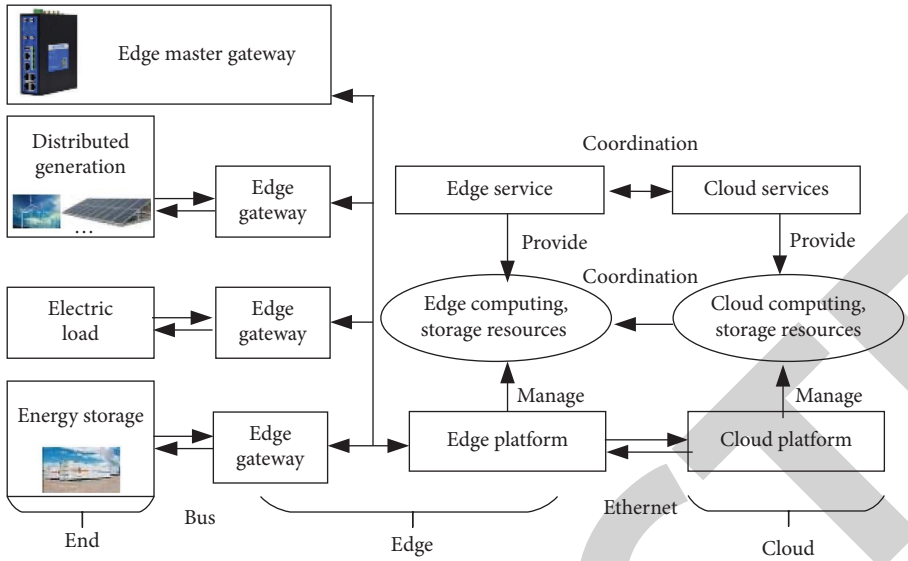

Figure 1: Microgrid architecture based on edge computing.

environment. The architecture design of the microgrid edge layer integrated with blockchain technology is shown in Figure 2.

Edge-computing servers are scattered in the edge environment of microgrid. In order to meet the requirements of data security processing at the edge layer, EdgeX Foundry edge-computing framework, Hyperledger Fabric blockchain, and trusted edge platform based on microservice architecture are deployed on the edge side.

Blockchain network can build a secure, trusted, and decentralized intelligent system in the edge environment. A blockchain network is jointly maintained by multiple edge server nodes. Each node, as a participant of the network, can communicate with other nodes on the blockchain network. Because the computing power of some terminal devices is limited, they cannot participate in the business of blockchain network. The proposed method uses the edge server to uniformly provide blockchain services for terminal devices; that is, all terminals complete identity authentication through the edge server and store it in the block [16]. After completing the identity authentication, the authorized terminal device can read the blockchain data but cannot write the data, which can effectively avoid data leakage. Users can access the edge server and edit smart contracts to create blockchain applications for terminal device needs. In the edge-computing architecture, the device identity, access control, and other information are stored by the blockchain, which can prevent the network information from being tampered with arbitrarily.

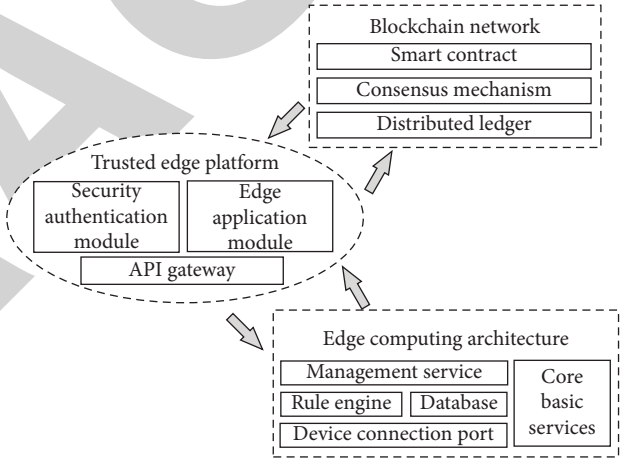

Figure 2: Design architecture of the microgrid edge layer integrated with blockchain technology.

3. Microgrid Security Defense Method Based on Edge Cooperation

For the edge-computing architecture for the microgrid, blockchain is deployed at the edge layer to build a blockchain system with multiple edge nodes, and security defense is carried out through the firmware layer, contract layer, and application layer. Using the edge cooperation mechanism based on the improved election algorithm, the leader node is selected from the edge nodes and the business channel is created. Then, based on the business requirements, we organize all nodes to edit and integrate the smart contract of full homomorphic encryption. After multiparty verification, the leading node will deploy it on the channel. Finally, multiple edge nodes in the channel cooperate according to the transaction process defined by the smart contract to fully realize the security defense of the microgrid.

3.1. Blockchain System with Multiple Edge Nodes. In the microgrid of multiedge-computing server, there will be frequent distributed two-way power and data communication; and the characteristics of blockchain technology, such as decentralization and encrypted transmission, just match it, which can ensure efficient, accurate, and global information interaction and sharing between multiedge nodes [17]. The blockchain interaction system with multiple edge nodes is shown in Figure 3.

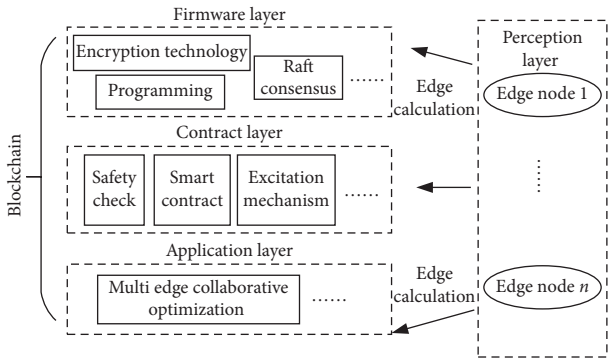

Figure 3: Blockchain interaction system with multiple edge nodes.

In the sensing layer of microgrid blockchain, different types of sensors and smart meters are arranged at decentralized nodes to collect and preprocess basic data. The data obtained in the sensing layer will be combined into a blockchain through encryption technology and consensus mechanism of the firmware layer, smart contract and incentive mechanism of the contract layer, and edge cooperation of the application layer [18].

3.2. Smart Contract Based on Homomorphic Encryption. If the edge node wants to access the data in the channel, it needs to go through the smart contract. After the smart contract performs identity authentication on the edge node, it encrypts the data in the channel by calling the SEAL homomorphism library and then transmits it to the edge node [19, 20]. After the identity of the edge node is fully homomorphic encrypted by the smart contract, the identity privacy of the edge node is ensured. The execution process of the smart contract at the edge is shown in Figure 4.

The edge client sends a request to the edge node Peer of Fabric. After receiving the request from the client, the edge node sends a request containing relevant requirements to the smart contract in the Docker container and executes the smart contract operation [21]. The smart contract executes the preset contract process and performs data operations on the status database. After receiving the smart contract instruction, the status database retrieves its status data and returns it to the smart contract. The status data are in a state that cannot be tampered with [22]. After receiving the read set of the status database, the smart contract performs the contract operation and performs homomorphic encryption on the status data and then returns the encrypted data to the edge node Peer.

Among them, the homomorphic encryption scheme contains four algorithms: key generation algorithm (KeyGen), encryption algorithm (Enc), decryption algorithm (Dec), and ciphertext calculation algorithm (Eval). In the process of homomorphic encryption, the key generation algorithm KeyGen (λ) is used to generate the decryption private key sk, encryption public key pk, and public key ek for ciphertext calculation, in which λ is the input security factor. The mathematical expression of KeyGen (λ) is as follows:

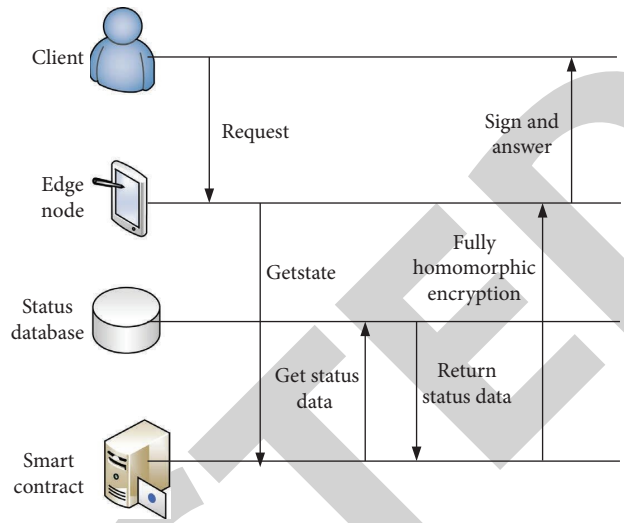

Figure 4: Edge smart contract execution process.

$$\begin{aligned} sk &= s, s \xleftarrow{\$} R_2, \\ pk &= \left(\left[-(as + e) \right]_q, a \right), \\ s &= sk, a \xleftarrow{\$} R_q, e \longleftarrow \chi, \\ ek &= \left(\left[-(a_i s + e_i) + \omega_i s^2 \right]_q, a_i \right), \\ a_i &\xleftarrow{\$} R_q, e \longleftarrow \chi, \end{aligned} \tag{1}$$

where χ is the integer distribution within the range, $s \xleftarrow{\$} R_2$, $a \xleftarrow{\$} R_q$ represents the process of uniform sampling, R is a polynomial, and ω is the base of logarithm.

Then, the encryption algorithm Enc(pk, m) is used to generate ciphertext c according to the input public key pk and plaintext m. For the same plaintext, the ciphertext obtained by each encryption is different. Assuming the plaintext $m \in R_t$, the public key is expressed as $pk = (p_0, p_1)$ and sampled as $e_1, e_2 \leftarrow \chi$. The ciphertext is calculated as follows:

$$c = \left(\left[\Delta m + p_0 u + e_1 \right]_q, \left[p_1 u + e_2 \right]_q \right), \tag{2}$$

where $\Delta = \lfloor q/t \rfloor$, q and t are coefficient modules of the ciphertext and plaintext, respectively, and u is the mask.

At the same time, using the decryption algorithm Dec(sk, c), the plaintext m can be obtained according to the input private key sk and ciphertext c. The calculation is as follows:

$$\begin{aligned} m &= \left[\left\lfloor \frac{t}{q} \left[c_0 + c_1 s \right]_q \right\rfloor \right], \\ c_0 &= c[0], c_1 = c[1]. \end{aligned} \tag{3}$$

Finally, the ciphertext calculation key ek, circuit $C(c_1, c_2, \cdots, c_k) \in C_\lambda$, and ciphertext $(c_1, c_2, \cdots, c_k)$ are input into the ciphertext calculation algorithm Eval(ek, $(c_1, c_2, \cdots, c_k)$,C), and the ciphertext calculation result c^* can be obtained.

3.3. Edge Cooperation Process Integrated with an Improved Election Algorithm. Due to the distributed characteristics of the microgrid, the deployed edge servers are independent of each other, and the decentralized architecture reduces the pressure on the central server. At the same time, due to the lack of centralized server organization, it is difficult for multiple nodes to cooperate to complete a certain task [23, 24]. EdgeX Foundry platform provides good interoperability locally. Therefore, an edge cooperation mechanism based on an improved election algorithm is proposed. Among them, a leading node is selected among multiple nodes through the election algorithm. The leading node creates a channel on the Hyperledger Fabric blockchain network and adds other member nodes to the channel.

The traditional election algorithm requires that each node in the system can communicate with each other, and it needs to obtain more than half of the votes to choose the master successfully. Therefore, the traffic is large and the election time is long. When a node obtains half of the votes, it is impossible to determine the leading node, resulting in the decline of the algorithm reliability. Therefore, in order to ensure the reliability of the election algorithm and speed up the election process, we integrate the trust model, and the nodes with the highest trust constitute the most valuable node set and carry out the election process [25]. Among them, the local credibility and global credibility in the credibility model and the local credibility p_{ij} are calculated as follows:

$$p_{ij} = \frac{S_{ij} - U_{ij}}{\sum_j S_{ij} - U_{ij}}, \tag{4}$$

where S_{ij} and U_{ij} are, respectively, the satisfaction times and dissatisfaction times accumulated by node i to node j in the historical transaction in a recent fixed time τ. The introduction of τ can realize the convergence problem of local credibility calculation, indicating that the algorithm pays more attention to the recent behavior of the nodes.

The calculation of global credibility is linear, that is, assuming that there are n nodes $i_0, i_1, \cdots, i_{n-1}$ in the whole universe and the relationship between them is $i_0 \longrightarrow i_1 \longrightarrow i_{n-1}$, then the global credibility T_{n-1} is as follows:

$$T_{n-1} = \sum_{i_1} \sum_{i_2} \sum_{\cdots} \sum_{i_{n-2}} P_{i_0 i_1} \times P_{i_1 i_2} \times \cdots P_{i_{n-2} i_{n-1}}. \tag{5}$$

In the election process, different proxy nodes may have the same trust degree, so the trust degree and the number are used to measure the value of the node, expressed as (d_i, ψ_i), where d_i is the number, which is the unique identification of the proxy node, and ψ_i is the trust degree. The trust level obtained from the trust rating in the global trust model is used to measure the value of the nodes. In this domain, the nodes regularly send probe messages to leaders and wait for the Reply message returned by the leaders [26]. If the node does not receive the Reply message from the leader within a predefined timeout interval, the election process is triggered. The election process is as follows:

(1) i send an Election message to the node in the set and wait for the ACK message of the corresponding node to detect whether the node exists.

(2) Nodes in the set perform the same operation to realize diffusion calculation, which will be carried out in a specific domain. Diffusion calculation is defined as follows:

If a node in the universe is currently participating in the diffusion calculation with index (d_1, ψ_1) and when it detects another diffusion calculation with higher priority and index (d_2, ψ_2), it will terminate the current diffusion calculation and participate in the diffusion calculation with index (d_2, ψ_2).

(3) If a node receives all ack messages except the nonexistent node in the neighbor node, it sends ACK messages to its upper node. This process will continue until i.

(4) i send a leader message to the nodes in the collection.

4. Experimental Results and Analysis

In the experiment, four Docker containers were started as the basic environment for virtual machine operation, and Docker containers were used as the operation environment of Hyperledger Fabric, including three as the edge point of the microgrid and one as the cloud center node, and fabric-chaincode-java was used to write smart contracts, as shown in Figure 5. At the same time, the data stored in the blockchain include the current and voltage values during the operation of the microgrid. See Table 1 for specific data. The whole safety protection system is in Ubuntu 16.04 (64 bit) virtual machine, Intel ® CoreTMit-4700HQ CPU @ 2.5 GHz processor, and 16G memory.

At the same time, the microgrid simulation model is built in the Matlab/Simulink environment, and the reference values of voltage and frequency are set as 380 V and 50 Hz, respectively, including three distributed generation (DG) and four loads. The relevant power settings are shown in Table 1.

4.1. Case Analysis. There are many types of network attacks. We take denial-of-service (DOS) attacks as an example to demonstrate the performance of the proposed method. Among them, the DoS attack types are Ping of Death, Teardrop, UDP FLOOD, SYN FLOOD, and Land Attack, and the attack times are set to 500, 350, 400, 280 and 190, respectively. The network intruder applies high-frequency DoS attack signals of the same frequency to the communication links between DG1 and DG2 and between DG2 and dg3. The changes of the reactive power ratio and the output voltage amplitude of each DG are shown in Figure 5.

As can be seen from Figure 6, the proposed method has strong resistance to high-frequency DoS attacks, which can ensure that the reactive power ratio still tends to be consistent and convergent under high-frequency DoS attacks. This is because when the DoS attack enters the sleep state, the proposed multiedge cooperation mechanism can ensure the successful information exchange between the edge nodes and will not cause network interruption due to the attack of the communication link so that the reactive power can be evenly distributed according to the DG capacity

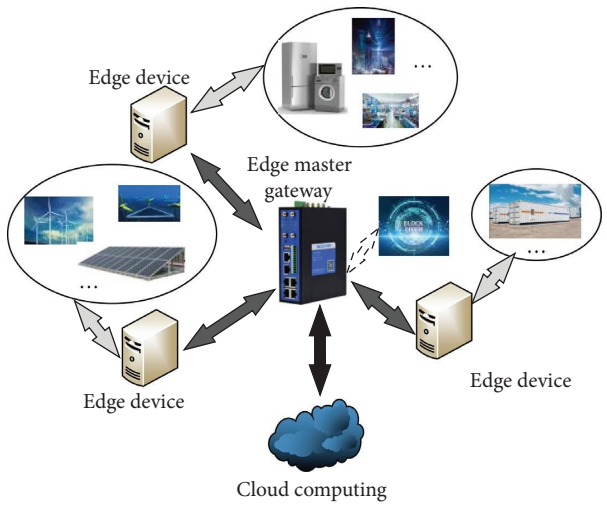

Figure 5: Schematic diagram of microgrid based on blockchain and edge computing.

Table 1: Parameters of microgrid-related equipment.

—	—	Power (kW)
DG	DG1	20
	DG2	15
	DG3	35
Load	L1	12
	L2	5
	L3	8
	L4	20

when the system reaches the steady state. At the same time, due to the network attack on the communication link, the voltage fluctuated briefly, but as the network detected the attack and isolated, the voltage soon stabilized. It can be seen that the proposed method can improve the safe and reliable operation ability of the microgrid system under DoS attack.

4.2. Performance Analysis of Edge-Computing Architecture. With the expansion of the scale of distributed generation, the number of microgrid devices and data increases sharply, and the edge-computing architecture can deal with massive data well. With the increase of computing nodes, the total access time of the proposed microgrid architecture is compared with that of the centralized-cloud architecture, as shown in Figure 7.

As can be seen from Figure 7, as the number of computing nodes increases, the total access time also increases. This is because when the edge node accesses the fabric channel database, the smart contract will homomorphically encrypt the data and the identity of the edge node. With the increasing number of edge nodes, the advantages of edge-computing mode are gradually reflected. Under the centralized-cloud architecture, when 40 computing nodes access data, the access time exceeds 3.7 s, and the computer CPU utilization reaches more than 90%. Under the edge-computing architecture, the access time decreases significantly with the increase of edge nodes. When the computing node is 40, the computer CPU utilization is about 70% under stable conditions, and the access time is only 2.5 s. This is because, under the edge-computing architecture, the edge node stores the data information generated at the edge in the local database, which greatly expands the storage space of the whole system. When accessing the local database, there is no need for consensus algorithm authentication, authentication, and data synchronization, and the amount of data on the blockchain network is significantly reduced, reducing the data flow and storage load of blockchain computing. Therefore, with the increase of the number of edge nodes, the advantages of edge-computing mode are more obvious, and the comparison and difference between the two modes are more and more obvious.

4.3. Stability Comparison of Different Methods. The proposed method has good defense capability against DoS network attacks. Based on this, the stability of the proposed method against various network attacks compared with the methods in [6, 9, 11] is analyzed. The results are shown in Figure 8. The evaluation standard is the change of current after the microgrid encounters a network attack.

It can be seen from Figure 8 that the proposed method has better stability, less current waveform burrs, and small fluctuations and tends to standard sine wave. Because the proposed method integrates edge-computing and blockchain technology, the data privacy is guaranteed through the designed smart contract, and the edge cooperation mechanism is constructed by using the improved election algorithm to further improve the security of the system. There are many burrs in the current waveform of other methods, and their resistance to network attacks is poor. Obert and Chavez [6] proposed a lightweight anomaly detection and graph theory method to protect potential threats in the power grid, but the protection performance of massive data is poor, and there are obvious burrs in the current waveform in the face of network attacks, and the peak value difference of current in each cycle is about 3A. Hasan et al. [9] apply blockchain technology to solve the security problem of the power grid, but the centralized protection mode is not suitable for microgrid, the current fluctuation is also obvious, and the peak difference in each cycle is close to 2A. Zhong and Xiong [11] established a security protection model of edge nodes based on non-cooperative differential games to ensure the security of edge nodes. Compared with [9], this method greatly improves the protection ability, but it lacks the consideration of edge cooperation and does not make good use of the relationship between the edges. Therefore, compared with the proposed method, the current waveform has more burrs and more obvious fluctuations.

4.4. Network Defense Success Rate of Different Methods. The proposed method is compared with the network defense success rate of the methods in [6, 9, 11]. The results are shown in Figure 9. The success rate of network defense is the ratio of the number of network attacks successfully defended to the total number of attacks.

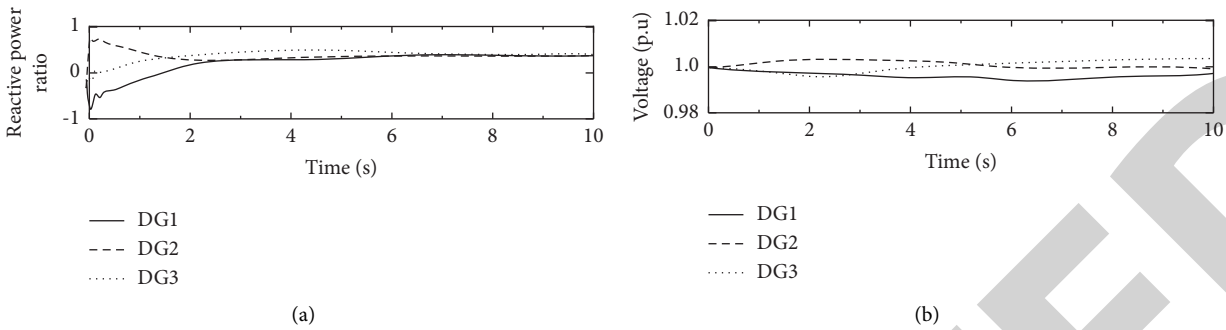

Figure 6: Security defense results under high-frequency DoS attack: (a) reactive power ratio; (b) voltage.

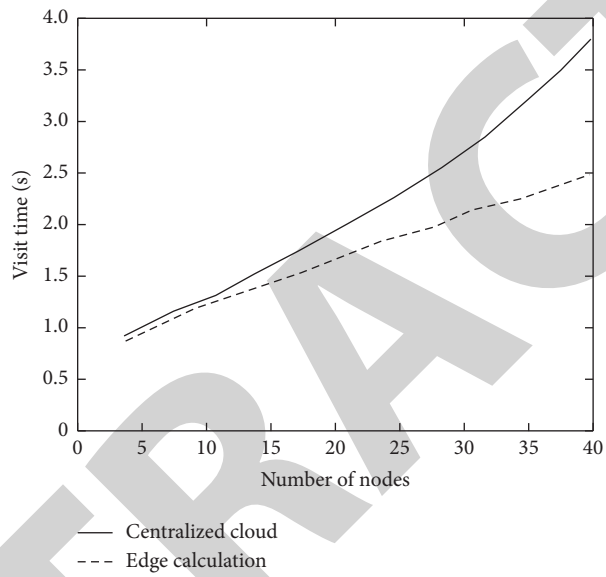

Figure 7: Calculation of the relationship curve between the number of nodes and the total access time.

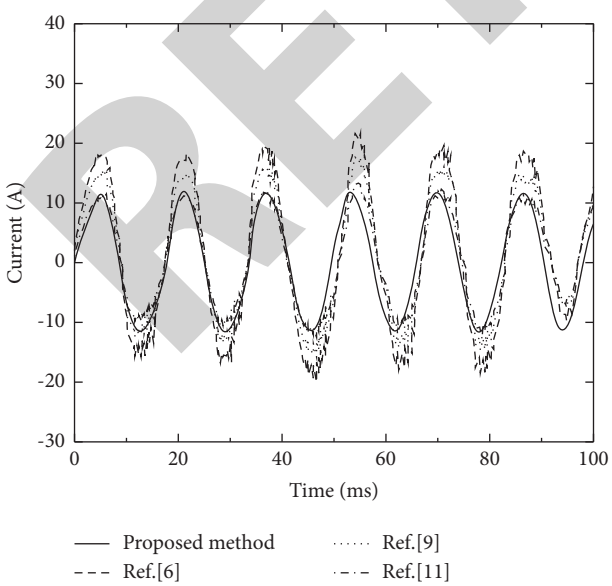

Figure 8: Stability comparison results of different methods.

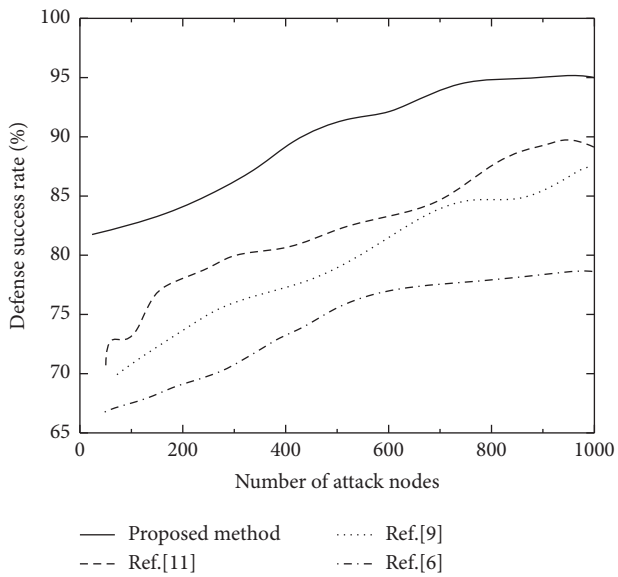

Figure 9: Comparison of defense success rates of different methods.

It can be seen from Figure 9 that the network attack defense success rate of the proposed method exceeds 95%. The integration of blockchain technology under the edge-computing architecture can not only improve the efficiency of data interaction but also ensure network security. In addition, the edge cooperation mechanism constructed by the election algorithm based on credibility can further improve the recognition performance of the system for network attacks, block detection, and defense one by one. The method in [6] is difficult to apply to microgrid architecture and cannot resist distributed network attacks, so the defense success rate is 80%. Both [9, 11] combine blockchain technology for network defense but lack the consideration of edge network characteristics, resulting in an unsatisfactory defense success rate of 90%. In conclusion, the proposed method has better stability and network defense ability, which can ensure the data interaction reliability of the microgrid.

5. Conclusion

Compared with the traditional centralized microgrid architecture based on cloud computing, edge computing overcomes the problems of the large transmission flow in the service process of cloud computing. However, the distributed characteristics of the microgrid lead to its security risks, which have gradually become the focus of attention. As a rapidly developing security technology in the recent years, blockchain has been widely used in many industries. Therefore, a microgrid security defense method based on cooperation in an edge-computing environment is proposed. The blockchain application is deployed on the edge side to provide security services for the network edge environment. And the homomorphic encryption algorithm is integrated into the smart contract to ensure data security. In addition, in order to improve the interoperability of edge-computing nodes, an improved election algorithm is used to build an edge cooperation mechanism to improve the ability to resist attacks. The results based on the microgrid simulation platform show the following:

(1) The application of edge-computing architecture can improve the efficiency of microgrid data processing. When the computing node is 40, the data access time is only 2.5 s, and the usage of computing memory is good.

(2) The microgrid security protection method based on edge cooperation can further improve the ability to resist attacks. When subjected to network attacks, its current fluctuation range is very small, and the defense success rate exceeds 95%.

Although the proposed method can meet the requirements in practical application, there are still some deficiencies, such as the complexity of the whole defense system. Therefore, the follow-up work will focus on the discussion of the blockchain lightweight consensus algorithm and the performance improvement of the trusted edge platform.

Data Availability

No datasets were used to support the findings of the study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. E. Ropp and M. J. Reno, "Influence of inverter-based resources on microgrid protection: Part 2: secondary networks and microgrid protection," *IEEE Power and Energy Magazine*, vol. 19, no. 3, pp. 47–57, 2021.

[2] A. B. Nassif, "A protection and grounding strategy for integrating inverter-based distributed energy resources in an isolated microgrid," *CPSS Transactions on Power Electronics and Applications*, vol. 5, no. 3, pp. 242–250, 2020.

[3] D. Lagos, V. Papaspiliotopoulos, G. Korres, and N. Hatziargyriou, "Microgrid protection against internal faults: challenges in islanded and interconnected operation," *IEEE Power and Energy Magazine*, vol. 19, no. 3, pp. 20–35, 2021.

[4] D. Ton, "Microgrid protection: R&D to meet the challenges to come [in my view]," *IEEE Power and Energy Magazine*, vol. 19, no. 3, pp. 107-108, 2021.

[5] P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Generation Computer Systems*, vol. 102, no. 3, pp. 902–911, 2020.

[6] J. Obert and A. Chavez, "Graph theory and classifying security events in grid security gateways," *International Journal of Semantic Computing*, vol. 14, no. 01, pp. 93–105, 2020.

[7] Y. Zhang and X. Zhao, "Key technologies of data security protection system for power grid," *Journal of Physics: Conference Series*, vol. 1656, no. 1, pp. 12024–12030, 2020.

[8] N. Suo and Z. Zhou, "Computer assistance analysis of power grid relay protection based on data mining," *Computer-Aided Design and Applications*, vol. 18, no. S4, pp. 61–71, 2021.

[9] M. K. Hasan, A. Alkhalifah, S. Islam et al., "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations," *Wireless Communications and Mobile Computing*, vol. 2022, no. 9, Article ID 9065768, 26 pages, 2022.

[10] O. Oksuz, "Providing anonymous communication, privacy-preserving data aggregation and dynamic billing system in smart grid using permissioned blockchain," *International journal of Network Security & Its Applications*, vol. 12, no. 2, pp. 17–36, 2020.

[11] J. Zhong and X. Xiong, "Data security storage method for power distribution internet of things in cyber-physical energy systems," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Article ID 6694729, 15 pages, 2021.

[12] 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. 1–20, 2020.

[13] L. Zhu, S. Peng, Z. Cai, W. Liu, C. He, and W. Tang, "Research on privacy data protection based on trusted computing and blockchain," *Security and Communication Networks*, vol. 2021, no. 12, Article ID 6274860, 9 pages, 2021.

[14] F. Tang, J. Pang, K. Cheng, and Q. Gong, "Multiauthority traceable ring signature scheme for smart grid based on blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Article ID 5566430, 9 pages, 2021.

[15] J. Gong and N. J. Navimipour, "An in-depth and systematic literature review on the blockchain-based approaches for cloud computing," *Cluster Computing*, vol. 25, no. 1, pp. 383–400, 2021.
[16] J. Gong and L. Zhao, "Blockchain application in healthcare service mode based on Health Data Bank," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 605–614, 2020.
[17] L. Campanile, M. Iacono, F. Marulli, and M. Mastroianni, "Designing a GDPR compliant blockchain-based IoV distributed information tracking system," *Information Processing & Management*, vol. 58, no. 2, pp. 1–23, 2021.
[18] S. K. Sharma, "A framework of big data as service platform for access control & privacy protection using blockchain network," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 476–485, 2021.
[19] N. Hettiarachchi and G. Pathiraja, "Blockchain based video conferencing system with enhanced data integrity protection auditability," *International Journal of Computer Application*, vol. 183, no. 16, pp. 20–25, 2021.
[20] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020.
[21] D. Wang, Y. Zhu, Y. Zhang, and G. Liu, "Security assessment of blockchain in Chinese classified protection of cybersecurity," *IEEE Access*, vol. 8, no. 4, pp. 203440–203456, 2020.
[22] O. Malomo, D. Rawat, and M. Garuba, "Security through block vault in a blockchain enabled federated cloud framework," *Applied Network ence*, vol. 5, no. 1, pp. 1–18, 2020.
[23] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: blockchain-based secure demand response management in smart grid system," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 613–624, 2020.
[24] J. S. Kim, J. S. Song, G. S. Shin, H. Y. Kim, and C. H. Kim, "Challenging issues and intelligent protective methods for microgrid protection," *The Transactions of the Korean Institute of Electrical Engineers*, vol. 70, no. 6, pp. 911–917, 2021.
[25] M. J. Reno, S. Brahma, A. Bidram, and M. E. Ropp, "Influence of inverter-based resources on microgrid protection: Part 1: microgrids in radial distribution systems," *IEEE Power and Energy Magazine*, vol. 19, no. 3, pp. 36–46, 2021.
[26] G. Le, Q. Gu, Q. Qu, Q. Jiang, and J. Fan, "AirCargoChain: a distributed and scalable data sharing approach of blockchain for air cargo," *Journal of Grid Computing*, vol. 18, no. 6-10, pp. 1–10, 2020.