Research Article

Power IoT System Architecture Integrating Trusted Computing and Blockchain

Yong Yan,1 Jinqian Chen,2 Ying Yao,1 Shaoyong Guo,1 Ao Xiong,2 and Wang Zhang2

1State Grid Zhejiang Electric Power Research Institute, Hangzhou, China 310014
2State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China 100876

Correspondence should be addressed to Jinqian Chen; chen_jinqian@bupt.edu.cn

Received 14 July 2021; Accepted 2 April 2022; Published 9 May 2022

Academic Editor: Chi-Hua Chen

Copyright © 2022 Yong Yan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the construction of power Internet of Things, the network scale is constantly expanding, the network structure is increasingly complex, and the number of terminals is increasing rapidly, resulting in huge pressure on network security protection, and it is urgent to build a credible operation environment to ensure that the Internet of Things runs safely and reliably. This paper proposes a power Internet of Things architecture combining trusted computing and blockchain. The architecture ensures the credibility and security of the terminal based on remote integrity verification and access control policy verification. A method for malicious node detection based on blockchain (MMNDB) is placed in acquisition layer. It is used to monitor the status of each acquisition devices in time, detect the malicious terminal in time, isolate the suspicious terminal with low credibility from the power Internet of Things, and ensure credibility of the acquisition terminal and the data collected. Under premise of ensuring the communication efficiency of the power communication network, this architecture can greatly ensure the stable working of the power Internet of Things.

1. Introduction

The definition of IoT was first proposed by Kevin Ashton [1], the founder of the Automatic Identification Center of the Massachusetts Institute of Technology. Currently, IOS/IEC defines IoTs as an infrastructure that connects people to things and information systems, on top of which are intelligent services capable of processing and responding to information. The Internet of Things is an information carrier based on the Internet, traditional telecommunications networks, etc. It enables all ordinary physical objects that can be independently addressed to form an interconnected network. At present, scholars have put forward the concept of ubiquitous power IoT. The ubiquitous Internet of Things revolves around the power system, making full use of information technologies to realize the power system’s interconnectedness of everything and everyone, forming a comprehensive state observation, efficient modern information processing, and application of intelligent services system. It is convenient and flexible [2].

In trusted computing, many organizations have different understandings of trust. ISO/IEC stresses the need to be resistant to a certain degree of virus and physical attack [3]. The IEEE definition emphasizes that it must be provable [4]. The Trusted Computing Group (TCG) defines trusted willfulness as follows: An entity is trusted if it always behaves in the expected way and toward the expected goal [5]. TCG’s trusted computing technology approach is to improve the security of computer systems by introducing a trusted platform module (TPM) on the hardware platform. This technology approach has been generally recognized by the industry. At the same time, the blockchain is a technology that allows a fully decentralized ledger to be created for transactions. All nodes in the network have access to its ledger. It is being used in an increasing number of fields [6–8].
Nowadays, the scale of network continues to expand, the network structure is increasingly complex, and the number of terminals has increased sharply. This has caused great pressure on network security protection. It is urgent to build a credible operating environment to ensure the network quality of the power Internet of Things and ensure the Internet of Things Safe and reliable operation of business. However, traditional trusted computing is used to solve the security problems of the architecture. It aims to establish a trust chain in computing system and extend trust relationship from the underlying hardware to the upper application to enhance the security of the computing system. The issue of trust in the data space also requires urgent attention. Decentralization is a feature of blockchain, and it can be used to solve the data space’s trust problem through a consensus method. As a result, it has become a development trend to integrate blockchain and trusted computing to build a high-credibility environment of physical networks and data logic spaces to support the construction of a trusted power Internet of Things.

The main contributions of this article are as follows:

(i) This paper proposes a power Internet of Things architecture that integrates blockchain and trusted computing. This architecture enables the device to have strong identity certification by deploying trusted chips in Internet of Things devices to ensure that the power Internet of Things has high-confidence characteristics. At the same time, the architecture achieves reliable data collection, secure transmission, reliable storage, and efficient use based on blockchain technology.

(ii) This paper proposes a method for detecting malicious nodes based on reputation. This method evaluates the credibility of power Internet of Things nodes from multiple dimensions and uses smart contracts to automatically execute malicious node detection algorithms, isolate malicious nodes in time, and ensure the stable and safe operation of power Internet of Things.

(iii) This paper designs a network quality evaluation model based on multidimensional evaluation indicators. The model uses a combined weight optimization model based on the least squares method to obtain the optimal weight value to assign the weight of the evaluation index, thereby improving the accuracy of the evaluation result.

(iv) According to the results of simulation experiments, the proposed strategy for detecting malicious nodes in this paper is more accurate, lower false alarm rate, and shorter detection time. At the same time, the power Internet of Things architecture proposed in this article can isolate malicious nodes in a timely manner after being attacked, maintain good network quality, and ensure the continuity of smart grid business.

2. Related Work

Different international organizations have provided different IOTS reference architectures, and their development has been widely recognized and used [9]. Traditional Internet of Things architecture employs a tiered system, which divides the Internet of Things into three layers: perception, network, and application. Comprehensive perception, dependable transmission, and intelligent processing are the features of the corresponding layer. Sensors, RFIDs, QR codes, and other information-gathering objects are found at the perception layer, as are smart devices and actuators for control; the network layer takes data from the perception layer and transfers it to the application layer, receiving a response from the application layer. The information will be routed and managed at the network layer, and the instructions will be passed to the perception layer; then there is another layer: The application layer contains middleware, application infrastructure, and numerous IoT services, with the purpose of providing interfaces for Internet of Things applications [10]. However, this traditional three-layer architecture does not build a credible operating environment and cannot well meet the requirements of power Internet of Things security protection.

Blockchain can be integrated with the Internet of Things to achieve decentralization and high accuracy of network resource management and access control, while ensuring data and identity privacy [11, 12], ensuring the stable operation of the Internet of Things system. The use of blockchain in the energy sector would increase energy security and efficiency by offering a distributed platform for systems, hence boosting the Internet of Things’ efficacy. People can immediately obtain energy information without the intervention of a third party, and real and high-quality data can be freely transmitted across devices. Furthermore, a blockchain-based IoT system aids the long-time running of smart grid devices [13]. There are still several issues with applying blockchain technology directly to the Internet of Things system due to a lack of sufficient computational resources and network bandwidth. At the same time, the security of blockchain nodes is also facing severe challenges.

For these reasons, some researchers have proposed to improve the overall security of related application systems by integrating blockchain with trusted computing.

Hybridchain is a solution presented by Wang et al. [14], which integrates blockchain with a TEE. Hybridchain can provide excellent performance while maintaining confidentiality. This technique, however, has yet to be successfully implemented in IoT applications.

In view of the problems of data privacy breach and difficulty in confirming data rights in the existing data transaction solutions, Zhang et al. [15] proposed a data transaction solution that combines blockchain and trusted computing technology with business requirements to build a new data transaction system. Compared with the traditional data transaction model, this solution uses the decentralized characteristics of the blockchain to store data index information, transaction process, and data usage records, which realizes the credibility and confirmation of data and
prevents data privacy. However, data transaction is too cumbersome and requires high performance on the blockchain and trusted computing platform; otherwise, it cannot meet the real-time demand for massive data transactions.

Gao et al. [16] integrated trusted computing and blockchain technology to propose a secure medical IoT data analysis framework, which adds the hardware-based software protection extension technology (SGX) in trusted computing to edge computing nodes. This technology can provide an encrypted trusted execution space in the memory for processing and analyzing medical data and storing analysis results. This part of the area is invisible to edge computing nodes, thus avoiding data leakage. The blockchain network of this framework is used to store data analysis results and result access control strategies to realize the credible use of data analysis results. However, the SGX technology used in this framework is based on Intel chips, which has compatibility and performance limitations. At the same time, it has high memory performance requirements for edge computing nodes.

Liu et al. [17] proposed a credible network architecture based on blockchain-B-TNC. B-TNC fully integrates the security features of blockchain decentralization, tamper-proof, and traceability and realizes a stronger network trust model. However, this method focuses on cross-domain network connection and is not suitable for interaction with IoT terminals.

In summary, preliminary work has been carried out on the integration of trusted computing and blockchain to build a high-credibility cyberspace and application system [18, 19]. However, it is still necessary to integrate trusted computing and blockchain to build a highly trusted power Internet of Things.

3. High-Credibility Power Internet of Things Architecture Integrating Trusted Computing and Blockchain

The high-credibility power Internet of Things architecture that integrates trusted computing and blockchain mainly include three parts: a trusted protection layer, a trusted power Internet of things layer, and a trusted data management layer. To solve potential data untrustworthiness of power IoT, this architecture adds a trusted chip to the collection terminal so that each collection terminal has a strong identity certificate. The trusted power Internet of Things layer works on top of the protection layer and ensures the credibility of data transmission and business applications in the Internet of Things through trusted terminals and trusted edge servers. The trust data management layer uses the blockchain to store the trust relationship and energy data of the collection terminal and uses the traceable and immutable characteristics of the blockchain to ensure that the trusted control data in the TPCM and the energy data in the Internet of Things are not illegally tampered with. Blockchain provides credible supervision of credible energy data and improves the sharing efficiency of credible energy data (see Figure 1).

The credible protection layer is the basis for ensuring the credibility of the entire power communication network architecture. The collection terminals and edge servers of the traditional power Internet of Things work in an open environment, so they are susceptible to various attacks, resulting in untrustworthy or leakage of energy data. In this architecture, the trusted platform control module (TPCM) is implanted in the collection terminal, edge server, and server of the blockchain node. It can achieve the credibility of the operating environment. TPCM builds a chain of trust when the terminal is started, tracks the log information recorded in the process of trust chain construction, and encapsulates the log information into transactions and uploads it to the blockchain as trusted control data. Each verifier can quickly pass the trusted control data. The correctness of the trust data is verified, the trust information of the terminal is effectively supervised, and the data is prevented from being maliciously tampered with.

The credible power Internet of Things network aims to extend the trust relationship from the collection terminal to the entire network. This architecture collects energy data through collection terminals with trusted chips, uses edge agents to filter invalid information, manages trusted energy data through the IoT management center and cloud system, and publishes energy data to the blockchain network. The trusted Internet of Things realizes the flexible recording of various trusted collection terminals and the interconnection of trusted energy data. At the same time, the data center can provide real-time data analysis and provide data sharing interfaces for other data applications, which greatly reduces the construction cost and technical complexity of the Internet of Things, and improve safety.

Data credibility management is mainly completed through the blockchain, which provides the entire architecture with trusted sharing of energy data and trusts computing security management. The blockchain stores the trusted control data of the TPCM. When a terminal is abnormal, or the control data is tampered with by an illegal attack, the blockchain can quickly find out the specific data through traceability. Moreover, deal with suspicious terminals to ensure the credibility of the credible power Internet of Things working environment. The efficiency of mass data sharing of traditional power Internet of Things is extremely low, and this architecture manages the energy data collected by the terminal through the blockchain and uses the decentralized characteristics of the blockchain to prevent the problem of major failure caused by the high concurrency of massive data. The use of the traceability feature of the blockchain to monitor trusted energy data prevents the problem of illegal data tampering that may exist in the traditional energy data center. At the same time, when a user application makes a data request, the data in the blockchain can be directly accessed. The need for cumbersome iterative requests and the coordination of data sources between different departments greatly simplify the processing process and improve the efficiency of the power Internet of Things.

3.1. Trusted Protection Layer. TPCM is the core component to ensure the credibility of network architecture calculations.
It is responsible for credibility measurement and protection of nodes. It can build a trusted system, prevent malicious access, and effectively avoid real-time attacks in the process of server running. As the root of trust of the system, TPCM supplements root of trust control function based on TPM to realize active control and measurement of the system.

When the system is initialized, TPCM will actively verify the BIOS before the CPU starts. After the verification is passed, the CPU can run, ensuring active control of the entire platform. TPCM will first evaluate the integrity of the entire system before all applications run and generate integrity values. When the program starts, the integrity measurement process checks the status of each application and module and saves the resultant integrity measurement value in PCR, which cannot be tampered with. The PCR log is kept by TPCM. TPCM uploads the data fingerprint obtained by calculating the PCR log data and other related information to the blockchain. The appropriate steps are as follows (see Figure 2):

1. Extract the data fingerprint of the previous PCR log information, and perform a hash operation together with this log information, user signature information, and user public key [3]

2. Transfer the data fingerprint of this log information obtained by the hash operation to the blockchain

The system administrator can use logs to ensure the validity of the integrity authentication process.

3.2. Data Trust Management. This section mainly introduces the high-credibility power information communication platform that integrates blockchain and trusted computing. After the platform is installed and deployed, it provides administrator control, asset management, and security policy configuration. The unified management of the host computer facilitates the operation of the administrator. At the same time, the security log of the host in the trusted computing environment is also collected, which is convenient for the administrator to view and manage.

As shown in Figure 3, the data trusted management platform can implement user management, log management, node management and other functions. User management controls administrator users, controlling user login, information modification, and user permissions. We can also use security options to strengthen the system’s own security from the system administrator identity, administrator use frequency, and password security. Node management is the unified management of hosts in a trusted computing environment, including node registration approval, whitelist scanning, allocation strategies, group management, modification of risk levels and groups, resetting node strategies, and deleting nodes. The platform can also collect security logs. The management center log performs auditing and log query functions of the administrator’s system operation behavior. The content of the log includes the administrator’s login, logout and all write operations. The node cluster log supports the auditing of event types and has a built-in default risk level.

4. Malicious Node Detection of High-Credibility Power Internet of Things

The architecture proposed a method of malicious node detection in the power IoT based on blockchain, which is called MMNDB. First of all, we introduce the data structure of the blockchain. The smart contract of the blockchain is designed in Sec. 4.2. This section presents the formal...
expression of the smart contract and discusses indicators of evaluating malicious nodes. Finally, the detailed process of malicious node detection is also expressed.

4.1. The Blockchain Data Structure for Detection of Malicious Nodes. In order to describe the blockchain for the detection of malicious nodes, this paper determines a block data structure based on blockchain for the detection of malicious nodes ($B_{bdmn} - BDS$). $B_{bdmn} - BDS$ records all data of communication.

Block header and block body are the two fundamental portions of a blockchain data structure, as shown in Figure 4. The block body contains the primary information of the power IoT gathering equipment, such as location, HMD, ID, PLR, MDR, CDR, and HBRT (see Sec. 4.2).

In a malicious node detection technology, the reputation of the collection terminal is evaluated in real-time from multiple angles. Check the terminals with low reputation value in time. Here, $T_1 - T_n$ represents each piece of equipment, Hash1 denotes the hash pointer of $T_1$ data, and Hash12 denotes the hash pointer of Hash1 + Hash2, resulting in a unique Merkle-root.

$B_{bdmn}$ employs a “block + chain” chain data structure, and it uses a Merkle Tree formed by a hash pointer to store the information acquired by each block. Once the data of any block is adjusted, such a data structure allows the hash pointer of the block to be changed. Furthermore, the data is recorded by various types of devices utilizing this data structure. When the entire network is freed, the risk of hostile manipulation is reduced, safety and fairness are ensured, and the detection process is made easier.

4.2. Smart Contract for Detection of Malicious Nodes. An expression for the smart contract is as follows:

$$B_{bdmn} - SC = (LS, ES, Sen, \theta, P, \sigma, LOC, TIM, HCD).$$ (1)
Among them, LS is generally trusted to deploy smart contract, ES is the server to execute contract, Sen is the collection device to be detected, $\theta$ is the assessment criteria, $P$ is reputation points, $\sigma$ is threshold of a node that is judged to be malicious, and LOC is the location of the device to be detected. TIM is timestamp of the message forwarded by the node. HCD is hash of control data of the node.

As shown in Figure 5, the steps are as follows:

Step 1. The LS deploys the smart contract $B_{bdmn} \rightarrow SC$.

Step 2. The LS authorizes the ES to execute the $B_{bdmn} \rightarrow SC$.

Step 3. In a trusted computing environment, (2)-(6) is used to calculate the communication information of collection equipment to obtain the corresponding $PLR$, $MDR$, $CDR$, and $HBRT$. These evaluation indicators will be stored in the blockchain periodically.

Step 4. The ES use the Judge() function of smart contract to check hash of control data (HCD), the timestamp, and location information of the terminal to be detected. If the control data is changed or the timestamp and location information is not as expected, the node can be judged to be malicious directly. Finally, the id of malicious nodes will be added to Set$_{id}$ of malicious nodes.

Step 5. The NodeCommunicationScore() uses the value of $PLR$, $MDR$, $CDR$, and $HBRT$ stored in the blockchain to calculate the CS value by (6).

Step 6. Compute the amount of $P$ using Formula (7).

Step 7. The ES uses the Detect() to cast the ID of malicious nodes as fellows: The system administrator sets threshold $\sigma$. When $P \leq \sigma$, the collection device is recorded to be malicious device. The id of this node will be added to Set$_{id}$ of malicious nodes.

Step 8. According to the Set$_{id}$ of malicious nodes, LS publishes malicious node information to the whole network by using consensus and isolates them from the credible network.

It is determined preliminarily that the current network is normal and the credible score value of the current network communication is calculated. The standards are expressed as follows:

$PLR = 1 - \left(\frac{n_{\text{recv}}}{n_{\text{send}}}\right)$, \hspace{1cm} (2)

where $n_{\text{recv}}$ presents number of packets successfully received. $n_{\text{send}}$ is the amount of data packets sent in the time period.

$MDR = \begin{cases} \left(\frac{T_{\text{sensor}}}{T_d}\right) \cdot T_d, & \text{if} \quad T_{\text{sensor}} \leq T_d; \\ 1, & \text{if} \quad T_{\text{sensor}} > T_d. \end{cases}$ \hspace{1cm} (3)

$CDR$: The response time required by malicious nodes is usually longer. The server notes the total time from receiving

Figure 4: Block data structure.
the request to the requester receiving the response from the node to be detected within a certain time interval.

\[ CDR = \frac{T_{hd} + T_{id}}{T_e}, \]

\[ T_{id} = Ms/Nb + \frac{pd}{ts}. \]  

Among them, \( T_{hd} \) is the time to process data. \( T_{id} \) is the time for message propagation, and \( Ms \) is the message size. \( Nb \) is network bandwidth. \( ts \) is the propagation speed, and \( T_e \) is the predetermined time period.

Historical behavior: The server calculates the proportion of malicious communication of the node to be detected in a certain time interval and uses this proportion as a reference standard for evaluating reputation:

\[ HBRT = \frac{Num_{MB}}{Num_{NB}} + \frac{Num_{MB}}{1}, \]  

where \( Num_{MB} \) is the number of malicious network communications. \( Num_{NB} \) represents the number of normal network communications.

CS of the device under test is as follows:

\[ CS = \lambda_1 \cdot PLR + \lambda_2 \cdot MDR + \lambda_3 \cdot CDR + \lambda_4 \cdot HBRT_T. \]  

Depending on the application context, each evaluation factor (\( \lambda \)) can be changed, and the sum of the evaluation factors needs to be 1.

The entire communication reputation \( P \) of the device under test is calculated by the overall amount of malicious network communication (\( N_{MB} \)) and the overall amount of normal communication \( N_{NB} \):

\[ P = e^{N_{NB}} / (e^{N_{NB}} + e^{N_{MB}} + 1). \]  

5. Simulation

To assess the method’s effectiveness of malicious node detection and the network architecture, the corresponding experiments are designed based on NS2. This paper used Ethereum to build \( B_{bdmn} \). The experiment evaluated the method’s effectiveness from several aspects, as shown in Table 1.

5.1. Detection Rate. When the number of total nodes is 80, the influence of the different numbers of malicious nodes on the detection rate is tested. There are 10 rounds of testing:

\[ \text{detection rate} = \sum N_{t_{mal}} / (N_{t_{total}} \times R). \]  

\( N_{t_{mal}} \) is the number of times that malicious nodes are detected in each round. \( N_{t_{total}} \) presents the number of total malicious nodes. \( R \) is the number of rounds.

In terms of the detection rate of malicious nodes, MMNDB and the approach proposed in [17] are compared in Figure 6. In the initial stage, the detection rates of the two scenarios are nearly identical, as seen below. As the simulation progressed, the number of malicious nodes in the network grew, and the figure shows that MMNDB has a greater detection rate than the technique in [17]. This is because the strategy described in this research uses more trustworthy data to detect malicious nodes. Furthermore, this article uses a combination of attributes to determine
whether or not a node is malevolent. When it comes to
detecting malicious nodes, MMNDB has a higher sensitivity.

5.2. False-Positive Rate. When the number of malicious
nodes is 20, the influence of the different number of total
nodes on the false-positive rate is tested. The false-positive
rate of the two methods is compared in Figure 7. There are
ten rounds of testing:

\[
\text{false positive rate} = \frac{\sum N_{fp}}{(N_{tmnd} \times R)}.
\]  

(9)

\(N_{fp}\) is the number of false positives. \(N_{tmnd}\) is the number of
times malicious nodes are detected in each round. \(R\) is the
number of rounds.

The chart demonstrates that at the initial simulation
stage, the false-positive rate is about the same. When the
total number of nodes reaches 60, the false-positive rate of
this technique is much lower than the algorithm in [17].
The false-positive rate of the algorithm in [17] increases dra-
matically as the number of total nodes grows. Because the
more nodes there are in the network, the more difficult it
is for the management system to monitor the behavior of
nodes. Then, the attacker can tamper with communication
data or detection algorithms easily. The normal nodes can
be defiled as malicious nodes by the attacker to destabilize
the network. However, MMNDB can ensure integrity of
communication evaluation data and credibility of detection
process based on blockchain. Therefore, this approach has
a lower false-positive rate than the comparison algorithm.
Moreover, it can ensure that the security and stability of
the network operation are better.

5.3. Detection Time. When the number of malicious nodes is
20, the number of total nodes is 80. The detection time of the
two methods is compared in Figure 8. As shown in the
figure, the number of malicious nodes in the power Internet
of Things decreases gradually with the increase of detection
time. However, the proposed method can detect more mali-
cious nodes simultaneously than [17]. Because the scheme
determines the node reputation from more dimensions, the
scheme has a higher detection accuracy. At the same time,
the scheme uses the smart contract method to automatically
execute the malicious node detection algorithm, which has a
higher execution speed and can detect and isolate the mali-
cious node in time.

5.4. Mean Throughput Speed. Throughput can be de-
\[\text{Mean Throughput speed} = \frac{\sum PR}{tsp - tst}.
\]

(10)

where \(\sum PR\) = size of the total receiving packet, \(tst\) = the start
time, and \(tsp\) = end time.

The throughput of different types of networks was tested
under the condition that malicious nodes were randomly
distributed with a probability of 30%, as shown in Figure 9.
As the number of nodes increases, the throughput increases.
However, the throughput of a network with malicious nodes

| Parameter                  | Value          |
|----------------------------|----------------|
| Simulation area            | 1000 m * 1000 m|
| MAC protocol              | 802.11DCF      |
| Initial battery power     | 10 J           |
| Transfer protocol         | UDP            |
| Packet size               | 1040 byte      |

| Number of malicious nodes | Detection rate |
|--------------------------|----------------|
| 2                        | 0.75            |
| 3                        | 0.80            |
| 4                        | 0.85            |
| 5                        | 0.90            |
| 6                        | 0.95            |
| 7                        | 1.00            |

| Number of total nodes    | False positive rate |
|--------------------------|---------------------|
| 40                       | 0.02                |
| 50                       | 0.04                |
| 60                       | 0.06                |
| 70                       | 0.08                |
| 80                       | 0.10                |
| 90                       | 0.12                |
| 100                      | 0.14                |

Figure 7: False-positive rate.
is the lowest. The throughput of network uses MMNDB that is affected by malicious nodes barely. Therefore, it can resist the attacks of malicious nodes on the network and ensure the efficient circulation of the network effectively.

5.5. End-to-End Latency. The overall time it takes for data to travel from the source to the destination is referred to as end-to-end latency, and it encompasses all of the numerous latencies experienced by the package from the sender to the receiver.

The average end-to-end latency (AEL) is as follows:

$$AEL = \frac{\sum (T_{pr} - T_{ps})}{N_{pr}}$$  \hspace{1cm} (11)$$

where $T_{pr}$ = time of receiving the package, $T_{ps}$ = time of sending the package, and $N_{pr}$ = number of received packages.

The end-to-end latency of different types of networks was tested under the condition that malicious nodes were randomly distributed with a probability of 30%, as shown in Figure 10. As the number of nodes increases, the latency of networks with malicious nodes increases sharply. However, the latency of the network uses MMNDB that is influenced by malicious nodes slightly. Therefore, it can reduce the negative effect of malicious nodes on the whole network effectively.

5.6. Package Delivery Rate. The package delivery rate (PDR) represents the success rate of packet transmission within a given time interval. It is as follows:

$$PDR = \frac{\sum N_r}{\sum N_g} \times 100,$$  \hspace{1cm} (12)$$

where $N_r$ = number of package received and $N_g$ = number of package generated.

The package delivery rate of different types of networks was tested under the condition that malicious nodes were randomly distributed with a probability of 30%, as shown in Figure 11. As the number of nodes increases, the package delivery rate decreases. However, the PDR of networks with malicious nodes goes down dramatically. Meanwhile, the network uses MMNDB to accurately isolate the malicious nodes to ensure that the packet loss rate is reduced efficiently.

5.7. Network Quality Evaluation. The evaluation index is the state parameter that reflects the quality of network service. Establishing evaluation indexes and building a network quality evaluation model can quantify the evaluation process, and the objective evaluation of network service quality can be achieved. In order to make the network service quality reference, this paper chooses the following evaluation indicators for research:

(1) Stability refers to the degree to which the measured values of various indicators in the network deviate from the normal values after being disturbed and affected. In this experiment, the stability of each service throughput needs to be calculated. The less the deviation, the better the stability of the network; otherwise, the worse the stability of the network. The specific calculation formula is as follows:

$$S = |X_i - \bar{X}|.$$  \hspace{1cm} (13)$$

$S$ denotes the system’s stability, $X_i$ is the measured value of each indicator, and $\bar{X}$ is the average measurement value of each indicator.

(2) Response time represents the time from the start of the request message from the IoT terminal to the end of service execution. It includes data transmission time, requests queuing time, system processing
subjective weight and objective evaluation indicators. At the moment, there are two types of weighting methods: subjective weighting and objective weighting. Subjective weighting reflects the preference of decision-makers, but subjective factors influence the results. Objective weighting is based on mathematical theory, but it ignores the preference of decision-makers. In order to effectively avoid the limitation of single weight, this paper adopts the combined weight optimization model based on the least square method to obtain the optimal weight value. We define grouping weights as \( \omega = (\omega_1, \omega_2, \cdots, \omega_n) \). The specific operations are as follows:

1. Subjective weight \( \mathbf{U} = (u_1, u_2, \cdots, u_n) \) can be determined by modified step analysis
2. Objective weight \( \mathbf{V} = (v_1, v_2, \cdots, v_n) \) can be determined using the improved G1 method
3. Lagrangian functions are constructed using least squares models:

\[
L(\omega, \lambda) = g(\omega) + \lambda \left( \sum_{j=1}^{m} (u_j - \omega_j)^2 + (v_j - \omega_j)^2 \right)
+ 4\lambda \left( \sum_{j=1}^{m} \omega_j - 1 \right).
\]

4. The optimal comprehensive weight was obtained by Lagrange function:

\[
\omega = A^{-1} \left[ B + \frac{1 - E^T A^{-1} B}{E^T A^{-1}} E \right].
\]

Among them:

\[
A = \text{diag} \left[ \sum_{i=1}^{m} z_{i1}^2, \sum_{i=1}^{m} z_{i2}^2, \cdots, \sum_{i=1}^{m} z_{im}^2 \right] \\
E = [1, 1, \cdots, 1]^T \\
B = \left[ \sum_{i=1}^{m} \frac{(u_i + v_i) z_{i1}^2}{2}, \cdots, \sum_{i=1}^{m} \frac{(u_i + v_i) z_{im}^2}{2} \right]^T. \\
\omega = [\omega_1, \omega_2, \cdots, \omega_n]. 
\]

The weighted standardized evaluation matrix is obtained by multiplying the optimal comprehensive weight and standardized evaluation index matrix:

\[
Y = \begin{bmatrix}
\omega_1 z_{11} & \omega_2 z_{12} & \cdots & \omega_n z_{1n} \\
\omega_1 z_{21} & \omega_2 z_{22} & \cdots & \omega_n z_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
\omega_1 z_{m1} & \omega_2 z_{m2} & \cdots & \omega_n z_{mn}
\end{bmatrix}. 
\]

Based on the weighted normalization matrix, this paper establishes a multi-attribute network quality evaluation model. The combined weight was calculated by MATLAB software. The combined weights are shown in Table 2.
The experimental process of network quality assessment is as follows:

(1) In the initial stage of the experiment, NS2 software was used to build the simulation network. The total number of IoT nodes in the IoT system was 100, including 30 malicious nodes and two servers. MQTT/CoAP protocol was used for communication between IoT nodes and servers. The FTP/HTTP protocol is used to transfer data between the Internet of Things client and server.

(2) In the experimental stage, two malicious nodes were added to the Internet of Things system every 5 minutes, and data was collected according to the evaluation indicators given in Figure 12. The network quality assessment model designed in this paper is used to evaluate the network quality between the network architecture that integrates blockchain and trusted computing technology and the traditional IoT architecture every 2 minutes. The results are shown in Figure 13.

As shown in Figure 13, with the increase of experiment time, the network quality of the two architectures increases.
gradually and eventually tends to be stable, but the network architecture proposed in this paper has better network quality.

5.8. Result Analysis. Based on the above simulation analysis results, under the same conditions, this paper proposed a malicious node detection method with higher accuracy compared with the literature [17], which can effectively guarantee the normal communication of the power Internet of Things. Meanwhile, this method has a lower false-positive rate and detection time. According to a network quality evaluation model, the quality of the proposed network architecture is tested. The test results show that the proposed network architecture can identify malicious nodes quickly and accurately, ensuring the stable operation of the power Internet of Things. The method proposed in this paper uses blockchain technology to store data of communication quality. The corresponding data must be obtained from the blockchain system during detection, so there are certain defects in detection efficiency. However, the method uses the trusted computing technology, which is complicated in function implementation and has disadvantages of poor compatibility.

6. Conclusion

The combination of trusted computing and blockchain technology can achieve trust transfer in trusted computing. However, the current blockchain has the disadvantages of low performance and high hardware requirements. Trusted computing also has the disadvantages of poor compatibility and slower computing speed. Therefore, no one has combined the applicable blockchain technology and trusted computing technology in the power Internet of Things. The high-credibility power Internet of Things architecture that integrates trusted computing and blockchain combines the benefits of trusted computing with the benefits of blockchain. It solves the problem of the centralization of former power IoTs and ensures the safety of every node based on trusted computing. The architecture is based on access control policy verification to ensure the security of terminal access. The existing malicious node detection methods [20–22] are mainly to realize the judgment by analyzing the node’s log, behavior, configuration, and other data. However, these data can easily be tampered with by attackers to conceal malicious behavior. As a result, the current method has the disadvantages of low detection rate, high false alarm rate, and long detection time. As a result, at the collection layer, a malicious node detection technique based on blockchain and reputation is designed. The low suspicious terminal is isolated from the high-credibility power information communication network, ensuring the credibility of the collection terminal. In conclusion, the high-credibility power Internet of Things architecture, which combines trusted computing and blockchain, dramatically improves system security while also maintaining the efficiency of power Internet of Things communication.

Although the system architecture proposed in this paper has many advantages above, it still has some defects. Considering the application scenarios comprehensively, the production of trusted computing chips usually needs to be adapted according to the different power equipment, which has poor compatibility and is difficult to be modified according to the application scenarios. At the same time, this architecture uses blockchain to store relevant data, which is insufficient in writing and reading. Therefore, in future work, the focus will be on improving the compatibility of the trusted computing platform and the efficiency of blockchain access.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work is supported by the Key Science and Technology Project of State Grid Corporation of China, No.5700202019374A0000.

References

[1] W. H. Hassan, “Current research on Internet of Things (IoT) security: a survey,” Computer Networks, vol. 148, pp. 283–294, 2019.
[2] R. Hou, G. Ren, C. Zhou, H. Yue, H. Liu, and J. Liu, “Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things,” Computer Communications, vol. 158, pp. 64–72, 2020.
[3] Common Criteria Project Sponsoring Organisation, Common Criteria for Information Technology Security Evaluation. ISO/
IEC International Standard 15408 Version 2.1, Common Criteria Project Sponsoring Organisation, Geneve, 1999.

[4] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[5] Trusted Computing Group, TCG specification architecture overview, version 1.2, 2003, 2011, https://www.trustedcomputinggroup.org.

[6] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, “A Blockchained federated learning framework for cognitive computing in industry 4.0 networks,” IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2964–2973, 2020.

[7] Y. Mu, F. Rezaeibagha, and K. Huang, “Policy-driven blockchain and its applications for transport systems,” IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 230–240, 2019.

[8] S. E. Chang and Y. Chen, “When blockchain meets supply chain: a systematic literature review on current development and potential applications,” IEEE Access, vol. 8, pp. 62478–62494, 2020.

[9] X. Sun, X. Zhang, Z. Xia, and E. Bertino, Artificial Intelligence and Security: 7th International Conference, ICAIS 2021, Dublin, Ireland, July 19–23, 2021, Proceedings, Part I. Vol. 12736, Springer Nature, 2021.

[10] H. Tran-Dang, N. Krommenacker, P. Charpentier, and D. S. Kim, “Toward the Internet of Things for physical internet: perspectives and challenges,” IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4711–4736, 2020.

[11] S. Sun, R. Du, S. Chen, and W. Li, “Blockchain-based IoT access control system: towards security, lightweight, and cross-domain,” IEEE Access, vol. 9, pp. 36868–36878, 2021.

[12] P. Danzi, A. E. Kalør, Č. Stefanović, and P. Popovski, “Delay and communication tradeoffs for blockchain systems with lightweight IoT clients,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2354–2365, 2019.

[13] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, “Blockchain in smart grids: a review on different use cases,” Sensors, vol. 19, no. 22, pp. 4862, 2019.

[14] Y. Wang, J. Li, S. Zhao, and F. Yu, “Hybridchain: a novel architecture for confidentiality-preserving and performant permissioned blockchain using trusted execution environment,” IEEE Access, vol. 8, pp. 190652–190662, 2020.

[15] Z. H. Xuewang, Y. I. Zijie, F. E. Jiaqi, Y. E. Caijin, and F. U. Kang, “Data trading scheme based on blockchain and trusted computing,” Journal of Computer Applications, vol. 41, no. 4, pp. 939–944, 2021.

[16] Y. Gao, H. Lin, Y. Chen, and Y. Liu, “Blockchain and SGX-enabled edge computing empowered secure IoMT data analysis,” IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15785–15795, 2021.

[17] M. Liu, Y. Shi, and Z. Chen, “Distributed trusted network connection architecture based on blockchain,” Journal of Software, vol. 8, pp. 2314–2336, 2019.

[18] Y. Yan, S. Tianhong, S. Guo, and S. Kang, “Power blockchain guarantee mechanism based on trusted computing,” in International Conference on Artificial Intelligence and Security, pp. 488–501, Springer, Cham, 2021.

[19] L. Liu, J. Yang, and W. Meng, “Detecting malicious nodes via gradient descent and support vector machine in Internet of Things,” Computers & Electrical Engineering, vol. 77, pp. 339–353, 2019.