Research Article

Trusted Computing and Privacy Protection Method for Computer IoT Nodes Based on Fuzzy Logic Blockchain

Beixin Zhong, Zilong Yang, Zhonghao Liu, Xiaoyong Chen, and Shi Cheng

1School of Information Science and Technology, Nantong University, Nantong, Jiangsu 226000, China
2Nantong Research Institute for Advanced Communication Technologies, Nantong, Jiangsu 226000, China

Correspondence should be addressed to Shi Cheng; chenshi@ntu.edu.cn

Received 23 June 2022; Accepted 1 August 2022; Published 31 August 2022

Copyright © 2022 Beixin Zhong 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 continuous growth of the social economy, the trusted computing and privacy protection methods of IoT nodes are constantly innovating and changing, from the traditional single IoT node protection method to the new interactive IoT nodes supplemented by various network resources. That is, the item information server encrypts the detailed information of the item layer by layer with the session key of the adjacent node according to the node sequence of the response path. By completing the complete interactive design and the protection knot in the unique illusory environment, the application and discussion of privacy protection is achieved in the context of Internet of Things, creating a design concept for trusted computing and privacy protection methods for IoT nodes, and discussing the rationality of interactive design in the process of trusted computing and privacy protection methods for IoT nodes. The simulation results show that the application of fuzzy logic blockchain is very extensive, and the trusted computing and privacy protection methods of IoT nodes have a broader platform and a more open environment.

1. Overview

The Internet of Things technology is closely related to people’s existing lives. In the process of collecting and quickly sharing environmental data, the Internet of Things has its own driving force for the rise of various industries. For example, smart cities arise from the needs of urban traffic flow control and social public services, and the growth of public infrastructure in connection with environmental data mining is caused by the urgent need to reduce energy costs, etc., but in addition to the use of the Internet of Things in major industries, the use of the Internet of Things in other fields also accounts for a large proportion, taking new engineering as the context of demand; colleges and universities are actively promoting the use of trusted computing and privacy protection for IoT nodes. Due to the poor autonomy of students in the protection process, the trusted computing and privacy protection methods of IoT nodes are not flexible enough, and the content of practicing IoT nodes trusted computing and privacy protection methods does not meet the existing needs of the industry. These are the common problems existing in the process of trusted computing and privacy protection methods for IoT nodes in current professional courses. In the practice of trusted computing and privacy protection methods for IoT nodes, it usually pays attention to the form but ignores the goals of trusted computing and privacy protection methods for IoT nodes. The amount of trusted computing and privacy protection methods is relatively small, and they are generally arranged after the protection of theoretical courses and cannot play a role in assisting the trusted computing and privacy protection methods of IoT nodes. In the practice of IoT node trusted computing and privacy protection methods, high repeatability exists, IoT node trusted computing and privacy protection methods are inefficient, and students’ individual development is not fully considered, which makes students gradually lose interest and initiative of protection, they are gradually disconnected from the social industry, and it cannot guide them to use their comprehensive abilities in the practice process [1–4].

In order to meet the actual needs of the current IoT node trusted computing and privacy protection methods, it is
necessary to correct the IoT node trusted computing and privacy protection methods for node trusted computing and privacy protection and use fuzzy logic blockchain to build node trusted computing and privacy protection methods [1, 5, 6]. Computing and privacy protection are required, in order to efficiently improve the quality of trusted computing and privacy protection methods for computer IoT nodes. This paper is based on fuzzy logic blockchain, by analyzing the trusted computing ideas and implementation methods of IoT nodes and integrates immersive protection into the specific privacy protection method, discussing the rationality of interaction design, to improve the trusted computing and privacy protection effect of IoT nodes [7–10].

2. Fuzzy Logic Blockchain Trusted Computing Method

The fuzzy logic blockchain mainly uses multiple constraints to improve the stability of the system. The essence of this method is to use multiple functional blockchains to effectively combine the obtained functional blockchain structures. Through the use of the original data samples, the obtained data is fed back to the sample data set. Suppose that the probability of each sample within the group can be extracted as

$$p = \left(1 - \frac{1}{N}\right)^N.$$  \hspace{2cm} (1)

In this paper, the fuzzy logic blockchain is used in the trusted computing and privacy protection design of the computer Internet of Things nodes, which can optimize the design of the functional blockchain and then improve the accuracy of the knowledge recognition of the constraint system. In the process of generating the borrowed blockchain, due to the independence of each blockchain, it can be processed in parallel, thereby effectively improving the efficiency of the system [11, 12]. The evaluation and analysis factors corresponding to the subject to be evaluated and analyzed are used as elements, and the abovementioned elements are used to construct an evaluation and analysis factor set for the design of trusted computing and privacy protection of computer Internet of Things nodes.

The design steps of trusted computing and privacy protection of computer IoT nodes are divided, and the set of evaluation and analysis factors is obtained:

$$\begin{align*}
U_1 & = \{U_{11}, U_{12}, \ldots, U_{1n}\}, \\
U_2 & = \{U_{21}, U_{22}, \ldots, U_{2n}\}, \\
& \vdots \\
U_m & = \{U_{m1}, U_{m2}, \ldots, U_{mn}\}.
\end{align*}$$

(2)

According to the top-down principle, various evaluation and analysis elements are divided into multiple levels, and the evaluation and analysis indicators are graded based on different levels and different systems combined with the attributes of the evaluation and analysis objects. Compare each index that exists at the same level, and quantify the comparison result according to the corresponding importance, and obtain the corresponding weight of the evaluation index of the trusted computing and privacy protection method of the computer Internet of Things node [13–15]. The specific steps are as follows.

Compared with the indicators present in this layer, a decision matrix $A$ is established, whose expression is as follows:

$$A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix},$$

(3)

$$b_{ij} = \frac{a_{mn}}{\sum_{i=1}^{n} a_{im}},$$

$$v_{ij} = \sum_{h=1}^{n} b_{ij}.$$

As the weight corresponding to the evaluation index of the privacy protection method of the Internet of Things node of the computer Internet of Things:

$$w_i = b_{ij} \cdot v_{ij} \cdot \frac{v_i}{\sum_{i=1}^{n} v_i}.$$  \hspace{2cm} (4)

According to the collected evaluation analysis data, the membership degree corresponding to the evaluation analysis index existing in the evaluation analysis element set is calculated, and the fuzzy matrix is constructed. $U_{mn}$

$$U_{mn} = \begin{bmatrix}
U_{11}, U_{12}, U_{13}, U_{14}, U_{15} \\
U_{21}, U_{22}, U_{23}, U_{24}, U_{25} \\
\vdots \\
U_{m1}, U_{m2}, U_{m3}, U_{m4}, U_{m5}
\end{bmatrix}.$$

(5)

$$I(S_1, S_2, \ldots, S_n) = \sum_{i=1}^{n} p_i \log_2(p_i).$$

In the formula, $p_i = |C_i|/|S|$ represents the probability of each sample being in the i-th class.

With the explosive growth of IoT device data increments, the problem of long waiting time for frequent exchange of noncritical data has aroused widespread concern. In response to this problem, this paper proposes a real-time blockchain noncritical data frequent exchange strategy (Real-time Exchange Strategy for Frequent Exchange of Noncritical Data with Blockchain, RES-FENDB) based on DCPN [16, 17].

In order to better record and evaluate the data exchange process, a noncritical data exchange block structure with credit indicators is proposed. Among them, each data exchange includes the initiator’s account (Initiator Identity, IID), the receiver’s account (Receiver Identity, RID), the current exchange of noncritical data items (Current Exchange of Noncritical Data, CEND), the initiator’s account normal data exchange record set (Normal Exchange Set,
NESP, and bad data exchange record set (BadExchangeSet, BES). The “high frequency, noncritical” mentioned in this article needs to meet the following two conditions at the same time:

1. \( \text{cend} \in (a, b) \), that is, \( \text{cend} \) is a nonkey data item. Among them: \( a, b \) are the measurement values of the noncritical data of the data.

2. \( \sum_{i=1}^{K} \text{Count}(\text{nes}_i + \text{bes}_i)/\text{period} > 50 \), that is, the total number of data exchanges per minute >50. Among them: \( \text{Count} \) is the counting function of the set; \( \text{nes}_i \) is the normal exchange set of the \( i \)-th initiator; \( \text{bes}_i \) is the bad exchange set of the \( i \)-th initiator; \( \text{period} \) is the time min used to complete the data exchange; \( K \) is the total number of initiators participating in the data exchange.

Therefore, based on the noncritical data exchange items, times, and bad data exchange sets of the originator, the data exchange characteristics and credit of the originator can be evaluated. This paper adopts the credit degree \( \alpha \) to reflect this dynamic credit status and uses the following mathematical strategies to evaluate \( \alpha \):

\[
p^\alpha_{ij}(t) = \begin{cases} 
\frac{a \times (t_{ij}(t))^\alpha \times \eta_{ij}(t)^\beta}{\sum_{h \in Q} 1/|t_{ij}(t)|^\alpha \times \eta_{ij}(t)^\beta}, & \text{if } j \in Q, \\
0, & \text{otherwise},
\end{cases}
\]

\[
\eta_{ij}(t) = \frac{1}{d_{ij}}.
\]

In order to take full advantage of the loop’s best solution and the best solution found so far, the pheromone of each computer IoT node is updated with each loop. The pheromone update rules are as follows:

\[
\begin{align*}
&\tau_{ij}(t + n) = (1 - \rho) \times \tau_{ij}(t) + \Delta \tau_{ij}(t), \\
&\Delta \tau_{ij}(t) = \sum_{k=1}^{m} \Delta \tau^k_{ij}(t).
\end{align*}
\]

It indicates the effect of the trusted computing and privacy protection method of the \( k \)-th computer IoT node, which remains on the network platform method in this calculation. \( \Delta \tau_{ij}(0) = 0, \Delta \tau^k_{ij}(t) \) represents the total amount of the above pheromone [22–24], as shown in Figure 2.

In the RES-FENDB strategy, if the receiver happens to be a full node in this type of blockchain, it has all the data exchange blocks of the initiator and can implement delay control and evaluate its credibility accordingly. The process of frequent exchange of noncritical data is relatively simple, and the meanings of the corresponding database places and transitions are shown in Table 1.

In the RES-FENDB strategy, if the receiver is a light node, it may not fully include the historical exchange data. At this time, the credit evaluation of the initiator should be done with the help of the verification node that
Figure 2: The process of frequent exchange of noncritical data of full nodes based on DCPN.

| Place/change | Meaning |
|--------------|---------|
| $s_{n1}$ | Transaction starts |
| $s_{n2}$ | The total exchange data of the initiator stored locally by the receiver |
| $s_{n3}$ | The total frequency of exchanges of the initiator stored locally by the receiver |
| $s_{n4}$ | Waiting for data exchange to complete |
| $s_{n5}$ | Both parties complete the data exchange |
| $s_{n6}$ | The whole network node judges whether the data exchange is legal |
| $s_{n7}$ | Block formation |
| $s_{n8}$ | Illegal exchange |
| $s_{f1}$ | Credits of initiator |
| $t_{d1}$ | The delay required for the data exchange to complete |
| $t_{o1}$ | The receiver conducts data exchange legality verification |
| $t_{o2}$ | Calculate the originator’s credit |
| $t_{o3}$ | The receiver publishes the transaction to the network |
| $t_{o4}$ | The accounting node is credited to the ledger |

Table 1: Place/transition meaning of frequent exchange of noncritical data of full nodes.

Table 2: Operational meaning of IoT node data exchange process.
has all the historical data. After the data exchange is completed, the joint verification of the entire network nodes should be carried out. If the receiver does not receive verification feedback during the block formation interval, it will be treated as an unoptimized situation. The meanings of the corresponding places and transitions are shown in Table 2.

Since it is most affected in the data exchange, it is necessary to ensure the security of the data after completing the data exchange. The RES-FENDB method can be used to quickly process the previous data exchange process, and the knowledge consensus can be used after the data exchange is completed. The method of data recording can effectively alleviate the risks caused by data exchange.

If the receiver is a full node, data exchange verification can be performed according to the historical data stored locally. Such nodes evaluate the credit of the initiator through the CF function and equations (5)–(7) and control the data exchange delay based on the delay control function DC and the suppression mechanism C. At the same time, this data exchange is broadcast to the network and implements final verification and accounting. For the vast majority of initiators without bad exchange records, this case can provide zero-delay data exchange services, which satisfies the need for frequent exchange of noncritical data in the blockchain; on the other hand, if the initiator is determined by the CF function as the low credit rating, it can only be exchanged through the traditional data exchange method; that is, it can only be carried out after the next block is formed.

If the receiver is a light node, a part of the initiator’s historical exchange data may be missing. At this time, the initiator’s ID can be broadcast to the network, and it can be verified by other verification nodes that have the initiator’s data exchange record. The specific verification method is the same as 2). In this verification method, the light node optimizes the data exchange speed through feedback from other nodes in the network. Considering that, in the actual blockchain network, most of them are light nodes, this strategy provides a feasible way to realize the frequent exchange of noncritical data among all nodes.

The above method actually improves the authentication efficiency by analyzing the historical credit of the originator and will inevitably face the threat of various illegal data exchanges (such as the double-spending problem). Faced with these threats, it can be effectively avoided by setting reasonable noncritical data measurement values, punishment mechanisms, and binding personal credit information. This paper chooses to set the measurement value and credit penalty mechanism of noncritical data. If there is an illegal data exchange, the accounting node will add this data exchange information to the bad data exchange transaction record set of the initiator.

This paper introduces the blockchain framework and proposes a smart home system based on Paillier encryption blockchain (PEB-SHS).

2.1. PEB-SHS Model

Definition 1. (smart home system based on Paillier encrypted blockchain) It is an octet, namely, PEB-SHS = (MT, HIG, SC, K, pkb, α, ϕ, β).

Among them, the meanings of MT, HIG, SC, α, and β are consistent with the SHS model, and K, pkb, and ϕ are

2.2. Block Data Model. In order to better describe the data form in the PEB-SHS model, this paper proposes a block data structure based on Paillier encryption (PE-BDS). Compared with the transaction data recorded by other blockchains, PE-BDS mainly records the user’s health information, such as BP, HR, RR, etc.

The largest feature of this data block is that it does not directly hash the collected information but first divides the plaintext information into two categories: visible information (public visible data, PVD) and invisible information (invisible privacy data, IPD). The former is some information that can be disclosed, while the latter is private, sensitive, and only user-visible information, such as BP, HR, RR, OC, etc. Then, use Block-PK to perform Paillier encryption on the IPD, and perform a hash operation with the visible information, and finally generate a unique Merkle-root for entry block header. The block body mainly records ciphertext information.

2.3. Privacy Protection Algorithm Based on Paillier Encrypted Blockchain. According to the PEB-SHS model described in the previous section, a privacy algorithm based on Paillier encrypted blockchain (the privacy protection algorithm based on Paillier encrypted block chain, P2A-PEBC) is further proposed. Specific steps are as follows:

1. Distribute the key SHK and the network-wide key BLOCK-PK. First, a pair of keys SHK is randomly assigned to each family high, and each pair of keys contains a pair of public key pki and private key ski. The whole network key BLOCK-PK consists of the public key pkb and the secret key skb.

2. Divide the nodes. Divide the entire network nodes into two categories; one is special nodes (Special Peer, SP), the number of which is at least 4 according to Byzantine consensus requirements, mainly storing K; the other is ordinary nodes (Normal Peer, NP), mainly responsible for publishing and verifying data information in the network.

3. Paillier encrypts IPD type data. First, the collected information is stored in the local HIG by the perceptron, and Paillier encryption is performed on the IPD with pkb; then the encrypted data and PVD are packaged together into a data package (DP), and ski is used for the signature or data packet.

\[ \text{DP} = \{\text{Data}_{ski} | d \in N^+, i \in N^+\}. \] (10)

Among them, \( d \) is the serial number of the data packet. Finally, HIG publishes the DPd to the network through the router.
3. Model Analysis and Experiment of Fuzzy Logic Blockchain

The three PCs are selected for test process of this paper, and the Apache JMeterVersion is taken as the tool to test the performance of this paper based on the fuzzy logic blockchain for a comparative analysis. Contrast and analysis are performed according to the round-robin algorithm, weighted round-robin algorithm, and the fuzzy logic blockchain method used in this paper in turn. The experiment mainly consists of two parts. The first part mainly conducts three sets of comparative tests. In the first set of experimental tests, three thread groups are constructed, and the number of threads is set to 10. In order to test the different types of access of trusted computing and privacy protection of computer IoT nodes in the actual operation process, there will be different degrees of system load. In the three thread groups, HTTP requests corresponding to different degrees of load are set in turn, and in the three thread groups, HTTP requests corresponding to different degrees of load are set in turn, and the thread load is set to 1, 5, and 10 in turn, and then the average corresponding response time and throughput of the platform are tested. During the three sets of tests, the number of threads was set to 100 and 500 in turn, and the settings of other blockchains were not changed. The experimental tests of the three groups are set to 150, 1500, and 9000. The experimental test results show that the running test results of the three algorithms can be compared within the set 9000 concurrency. In this case, compared to the polling algorithm, there is no competitive advantage. Since the weighting method takes a long time, the calculated time duration is 7 ms, which is 5.67 ms longer than the polling calculation method, and the number of jobs is roughly the same; it is obtained from the data that when the number reaches 9000, the calculation time of smooth calculation is less than that of polling calculation, which provides better work results. Three sets of experiments were selected to use dynamic calculation methods. The polling calculation and smooth weighted calculation were longer than the average corresponding time. At the same time, the throughput was also greater than the previous results. When the functions in the server were similar, the number of connections could better display the load data. Meanwhile, there is no tedious calculation time. The fuzzy logic blockchain proposed in this paper can better reflect the average efficiency and throughput, which confirms that dynamic load data can achieve ideal results in a complex network background.

During the construction of the data information base of the IoT node, the credibility of the path needs to be verified. Only after the credibility verification process is ensured, the corresponding data can be accessed, which can effectively increase the credibility of data storage process in Table 3. The project of data transmission in the IoT node needs to use the platform module as the guarantee of the security mechanism, and at the same time, the credibility of the access response path of the IoT node is verified to ensure that this paper builds a credible response path and enhances the credibility of the transmission of item information.

In this paper, MATLAB simulation program is used to construct the RES-FENDB strategy, and a simulation experiment is carried out on a small transaction process to verify its effectiveness. Assumption: Retailer Bob and the initiators Alice, Bill, and other 5 people are conducting small transactions, the transaction amount is less than 200 RMB (about 0.0208333 Bitcoin), and the transaction verification is carried out by Bob and 9 other retailers (10 nodes in total) as a validator node. Among them, the historical transaction data of the initiator owned by these 10 verification nodes are shown in Table 4, K is the total number of transactions, M is the total transaction amount, and NULL means that the node does not store this information.

10 rounds of simulations were performed on 5 transactions, and the time between the start of each transaction and the formation of the next block is shown in Table 5. Let $\alpha$, $\xi$, and $\sigma$ in the DCPN model be 8, 5, and 1.5, respectively. According to the formula, the credit rating $\alpha$ of the initiator given by each node can be obtained by calculation, as shown in Table 6.

Using the RES-FENDB strategy for small transactions, the transaction delay value of each round of simulation is shown in Table 7. Considering the network delay in real transactions, this experiment introduces network delay when simulating the transaction process and takes random numbers as 0.21587, 0.76817, 0.16967, 0.57892, 0.82071, 0.68045, 1.26064, 0.77601, 0.55335, and 0.34181. The RES-FENDB strategy is used to conduct small transactions with network transmission delay variables. The transaction delay value of each round of simulation is shown in Table 8.

From the conventional transaction method of the blockchain, the confirmation of the transaction needs to be realized after a new block is formed. Therefore, each transaction shown in Table 5 can be regarded as its confirmation waiting time until the next block is formed. Using the RES-FENDB strategy for small transactions (referred to as RES-FENDB (A)) will confirm a large number of transactions with high credit in advance, avoiding most unnecessary waiting (as shown in Table 7). The transmission delay variable is integrated into the RES-FENDB strategy (referred to as RES-FENDB(B)), which depicts the further fitting of the RES-FENDB strategy to the actual transaction data in the real trading environment (as shown in Table 8).

Further comparison and analysis of Tables 5–8 show

\[ \forall t \in T \rightarrow \max (D_{IA}(t), D_{IB}(t)) \leq D_{ref75}(t). \quad (9) \]

In the formula, $T$ is the set of all transaction items in a round of transactions, DIA, DIB, and Dref75 are RES-FENDB (A), RES-FENDB (B), and transaction delay, respectively. That is, in the small-value transactions (RES-FENDB(A) and RES-FENDB(B)) after applying the DCPN model, regardless of whether the network delay is considered, the delay of each transaction must be no greater than the transaction delay.

The total delay comparison of multiple rounds of transactions is shown in Figure 3. Compared with the conventional transaction process of the blockchain, the RES-FENDB strategy is endorsed by the credit of the initiator, which effectively improves the efficiency of transaction
### Table 3: Results of three groups of comparative experiments.

| Algorithm                        | Thread count | Concurrency | Average response time/ms | Throughput | Error rate |
|----------------------------------|--------------|-------------|--------------------------|------------|------------|
| **Polling algorithm**            |              |             |                          |            |            |
| 10                               | 100          | 5.67        | 56.50                    | 0          |
| 100                              | 1600         | 110.33      | 278.87                   | 0          |
| 500                              | 8000         | 533.00      | 323.77                   | 0          |
| **Weighted polling algorithm**   |              |             |                          |            |            |
| 10                               | 100          | 7.00        | 56.99                    | 0          |
| 100                              | 1600         | 180.33      | 197.93                   | 0          |
| 500                              | 8000         | 533.00      | 323.77                   | 0          |
| **Algorithm proposed in this paper** |        |             |                          |            |            |
| 10                               | 100          | 3.00        | 57.95                    | 0          |
| 100                              | 1600         | 74.00       | 326.17                   | 0          |
| 500                              | 8000         | 367.33      | 468.78                   | 0          |

### Table 4: Initiator information stored by Bob and the verification node.

| Validating node | Initiator (k/time, M/bitcoin) |
|-----------------|-------------------------------|
| Bob             | (53,2654)                     |
| Node 1          | NULL                          |
| Node 2          | (68,3457)                     |
| Node 3          | (80,4036)                     |
| Node 4          | NULL                          |
| Node 5          | (17,795)                      |
| Node 6          | (22,1034)                     |
| Node 7          | (7,279)                       |
| Node 8          | (73,3770)                     |
| Node 9          | (68,3457)                     |

### Table 5: The time from each transaction to the formation of the next block.

| Rounds       | Alice | Bill | Mark | Joan | Niki |
|--------------|-------|------|------|------|------|
| Round1       | 3.5414| 7.80769| 6.92872| 3.57067| 5.62259|
| Round2       | 6.86823| 4.72783| 5.68148| 4.99286| 3.21868|
| Round3       | 0.37521| 7.35936| 6.30589| 3.64826| 7.83015|
| Round4       | 4.43668| 6.27526| 5.70482| 3.88959| 2.68462|
| Round5       | 2.78827| 5.71848| 1.04911| 7.71653| 3.34502|
| Round6       | 5.69111| 4.74950| 2.48020| 1.79111| 7.19193|
| Round7       | 3.11460| 4.67285| 3.67830| 6.49002| 1.41369|
| Round8       | 3.80903| 8.86701| 3.28704| 1.57673| 7.39993|
| Round9       | 2.32376| 6.71490| 5.38392| 0.72566| 6.70171|
| Round10      | 7.08755| 5.88250| 2.03875| 9.93886| 2.04242|

### Table 6: Credits of each initiator.

| Validating node | Alice | Bill | Mark | Joan | Niki |
|-----------------|-------|------|------|------|------|
| Bob             | 0.60655| NULL| 0.19099| NULL| NULL|
| Node 1          | NULL| 0.67334| 0.59754| 0.80887| 0.87398|
| Node 2          | 0.74394| 0.01243| NULL| 0.80887| 0.00626|
| Node 3          | 0.80879| 0.06765| NULL| 0.62195| 0.87398|
| Node 4          | NULL| 0.72451| 0.85353| 0.20675| 0.43024|
| Node 5          | 0.08352| 0.01243| 0.08645| 0.02133| 0.87398|
| Node 6          | 0.14239| 0.01243| NULL| 0.36076| 0.00626|
| Node 7          | NULL| 0.35659| 0.44967| 0.56303| 0.43024|
| Node 8          | 0.77812| 0.01243| NULL| 0.56303| 0.57468|
| Node 9          | 0.74394| 0.22647| 0.02575| 0.68034| 0.57468|
verification. Its transaction delay can be reduced by 50%–75% compared with the conventional transaction process.

4. Discussion

Compared with traditional node trusted computing and privacy protection, the node trusted computing and privacy protection of fuzzy logic blockchain can provide users with protection resources, and the virtual reality IoT node trusted computing and privacy protection methods are analyzed through the network. The fuzzy logic blockchain can be used to intelligentize and virtualize the protection content of IoT nodes, enabling users to analyze private content and realize user interaction. Users can quickly access the trusted computing and privacy protection method resources of IoT nodes through the computer Internet of Things, thereby

**Figure 3: Comparison of total transaction delays.**

**Table 7: Transaction delay under RES-FEMDB/min.**

| Rounds | Alice    | Bill     | Mark   | Joan    | Niki     |
|--------|----------|----------|--------|---------|----------|
| DI_1   | 3.54414  | 0        | 0      | 0       | 5.62259  |
| DI_2   | 6.86712  | 0        | 0      | 4.99165 | 0        |
| DI_3   | 0        | 7.35849  | 6.30477| 0       | 7.82953  |
| DI_4   | 0        | 5.70371  | 3.88766| 0       | 0        |
| DI_5   | 2.78827  | 0        | 1.04911| 7.71653 | 3.34502  |
| DI_6   | 5.69111  | 4.74950  | 0      | 0       | 0        |
| DI_7   | 3.11460  | 0        | 0      | 6.49002 | 1.41369  |
| DI_8   | 0        | 0        | 3.28704| 1.57673 | 7.39993  |
| DI_9   | 0        | 0        | 0      | 0.72566 | 0        |
| DI_10  | 0        | 5.88250  | 0      | 0       | 2.04242  |

**Table 8: Transaction delay of RES-FEMDB with network transmission delay.**

| Rounds | Alice    | Bill     | Mark   | Joan    | Niki     |
|--------|----------|----------|--------|---------|----------|
| DI_1   | 3.76001  | 0.21587  | 0.21587| 0.21587 | 5.83846  |
| DI_2   | 7.63529  | 0.76817  | 0.76817| 5.75982 | 0.76817  |
| DI_3   | 0.16967  | 7.52816  | 6.67444| 0.16967 | 7.99920  |
| DI_4   | 0.57892  | 0.57892  | 6.28263| 4.46658 | 0.57892  |
| DI_5   | 3.60898  | 0.82071  | 1.86982| 8.53724 | 4.16573  |
| DI_6   | 6.37156  | 5.42995  | 0.68045| 0.68045 | 0.68045  |
| DI_7   | 4.37500  | 1.26064  | 1.26064| 7.75066 | 2.67433  |
| DI_8   | 0.77601  | 0.77601  | 4.06305| 2.35274 | 8.17594  |
| DI_9   | 0.55335  | 0.55335  | 0.55335| 1.27901 | 0.55335  |
| DI_10  | 0.34181  | 6.22431  | 0.34181| 0.34181 | 2.38423  |
realizing the independent protection of resource information.

5. Conclusion

With the continuous development of Internet of Things technology, node trusted computing and privacy protection have gradually been paid attention to. In response to these needs and deficiencies, on the basis of fuzzy logic blockchain, immersive privacy content analysis can be performed from a traditional perspective, allowing users to experience specific privacy content, fully mobilizing users’ enthusiasm, and improving IoT node trusted computing and the specific quality and effectiveness of privacy-preserving methods. By analyzing the business logic of trusted computing and privacy protection of IoT nodes, using the linkage between computer IoT and users, it breaks the space and time of traditional protection methods, allowing users to complete the protection of privacy content anytime and anywhere. Implement interaction design and fuzzy logic blockchain, and implement analysis in specific applications and interaction design. The simulation results show that the trusted computing and privacy protection method of computer Internet of Things nodes can enable users to immerse themselves in the privacy protection content more actively and master the privacy content. Compared with the traditional Internet of Things transmission mechanism, the improved Internet of Things information transmission mechanism is more suitable for the current complex network environment.

Data Availability

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

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] P. Maene, J. Gotzfried, R. de Clercq, T. Muller, F. Freiling, and I. Verbauwhede, “Hardware-based trusted computing architectures for isolation and attestation,” IEEE Transactions on Computers, vol. 67, no. 3, pp. 361–374, 2018.

[2] L. Rossi, E. Carbonieri, C. Castello, R. Rossi, G. Sciarretta, and P. Zardini, “Description and evaluation of a method for computer analysis of the exercise electrocardiogram,” Journal of Electrocardiology, vol. 20, no. 5, pp. 312–320, 1987.

[3] Mylonakis, Damianos, and Papaefstathiou, “Node.DPWS efficient web services for the internet of things,” IEEE Software, vol. 4, no. 5, pp. 1–10, 2016.

[4] B. Zheng, D. Gur, W. F. Good, and L. A. Hardesty, “A method to test the reproducibility and to improve performance of computer-aided detection schemes for digitized mammograms,” Medical Physics, vol. 31, no. 3, pp. 2964–2972, 2004.

[5] D. S. Gorman and J. S. Connolly, “A method for computer analysis of kinetics of competing first- and second-order reactions,” International Journal of Chemical Kinetics, vol. 5, no. 6, pp. 977–989, 1973.

[6] A. Grzybowski and A. BRóADKA, “Lekner type method for summing the dipole—dipole interactions in computer simulations of one- and two-dimensionally periodic systems,” Molecular Physics, vol. 101, no. 8, pp. 1079–1088, 2003.

[7] C. J. Ewart, C. J. Leonard, J. G. Harper, and J. Yu, “A simple and inexpensive method of preoperative computer imaging for rhinoplasty,” Annals of Plastic Surgery, vol. 56, no. 1, pp. 46–49, 2006.

[8] L. H. Yin, L. N. Xu, X. N. Wang, B. N. Lu, Y. T. Liu, and J. Y Peng, “An economical method for isolation of dioscin from Dioscorea nipponica makino by HSCCC coupled with ELSD, and a computer-aided UNIFAC mathematical model,” Chromatographia, vol. 71, no. 1–2, pp. 15–23, 2010.

[9] D. J. Bacon and N. A. Geary, “Computer simulation of polyethylene crystals. I. Method, structure and elastic constants for perfect crystals,” Journal of Materials Ence, vol. 18, no. 3, pp. 853–863, 2018.

[10] M. Lucas, “Method and apparatus for voice dictation and document production,” Journal of the Acoustical Society of America, vol. 118, no. 3, pp. 1259–1269, 2018.

[11] A. S. Yoon, “Method and apparatus for controlling a sound function of a computer system,” Journal of the Acoustical Society of America, vol. 118, no. 4, pp. 2105–2114, 2016.

[12] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, “Big data privacy preserving in multi-access edge computing for heterogeneous internet of things,” IEEE Communications Magazine, vol. 56, no. 8, pp. 62–67, 2018.

[13] S. Wang, H. Wang, J. Li et al., “A fast CP-abe system for cyber-physical security and privacy in mobile healthcare network,” IEEE Transactions on Industry Applications, vol. 4, no. 9, pp. 1–6, 2020.

[14] Elhaddad, Mohamed, and Bog, “The multi-level hp-method for three-dimensional problems: dynamically changing high-order mesh refinement with arbitrary hanging nodes,” Computer Methods in Applied Mechanics and Engineering, vol. 310, no. 10, pp. 252–277, 2016.

[15] K. K. R. Choo, Z. Tan, X. He, J. Hu, and T. Qin, “Ieee access special section editorial: security and trusted computing for industrial internet of things: research challenges and opportunities,” IEEE Access, vol. 8, no. 3, pp. 145033–145036, 2020.

[16] L. Cai, S. Yang, Z. Chen, Y. Pan, and M. Xu, “A decentralized and trusted edge computing platform for internet of things,” IEEE Internet of Things Journal, vol. 101, no. 8, pp. 1079–1088, 2019.

[17] H. Qian, “Research on the internet of things information transmission protocol based on trusted computing,” Wireless Internet Technology, vol. 56, no. 1, pp. 46–49, 2018.

[18] Y. Wang, W. Huang, J. Yu, K. Chen, and F. Wang, “Data privacy protection method of internet of things based on blockchain technology,” Journal of Physics: Conference Series, vol. 1651, no. 1, 23 pages, Article ID 012068, 2020.

[19] Z. X. Nie, Y. Z. Long, S. L. Zhang, and Y. M. Lu, “A controllable privacy data transmission mechanism for internet of things system based on blockchain,” International Journal of Distributed Sensor Networks, vol. 18, no. 3, 863 pages, Article ID 155013292201084, 2022.

[20] S. Simaiya, U. K. Lilhore, S. K. Sharma, K. Gupta, and V. Baggan, “Blockchain: a new technology to enhance data security and privacy in internet of things,” Journal of
[21] A. Nayeem, F. Shafiq, M. Aftab, R. S. Pirzada, and S. Ghazala, “Comparison of security challenges and issues of mobile computing and internet of things,” vol. 20, no. 5, pp. 312–320, 2018.

[22] M. Yu, J. Zhang, J. Wang et al., “Internet of things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain,” International Journal of Distributed Sensor Networks, vol. 14, no. 12, 10 pages, Article ID 155014771881584, 2018.

[23] X. Zhang, Z. Cao, and W. Dong, “Overview of edge computing in the agricultural internet of things: key technologies, applications, challenges,” IEEE Access, vol. 8, no. 3, pp. 141748–141761, 2020.

[24] C. Shen, “On the development trend of trusted computing and intellectual property protection,” China Invention & Patent, vol. 5, no. 6, pp. 977–989, 2019.