Mathematical Biosciences and Engineering

MBE, 19(4): 4196–4216.
DOI: 10.3934/mbe.2022194
Received: 16 December 2021
Revised: 09 February 2022
Accepted: 13 February 2022
Published: 18 February 2022

http://www.aimspress.com/journal/MBE

*Research article*

# Zero trust in edge computing environment: a blockchain based practical scheme

**Dawei Li[1,2,*], Enzhun Zhang[1], Ming Lei[3] and Chunxiao Song[1]**

[1] School of Computing Engineering, Nanjing Institute of Technology, Nanjing 211167, China
[2] Energy Research Institute, Nanjing Institute of Technology, Nanjing 211167, China
[3] NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China

* **Correspondence:** Email**:** lidw@njit.edu.cn.

**Abstract:** Edge computing offloads the data processing capacity to the user side, provides flexible and efficient computing services for the development of smart city, and brings many security challenges. Aiming at the problems of fuzzy boundary security protection and dynamic identity authentication in the edge computing environment in smart city, the zero trust architecture based on blockchain is studied, and a digital identity model and dynamic authentication scheme of edge computing nodes based on distributed ledger are proposed. Firstly, a digital identity model of two-way authentication between edge computing node and sensing terminal is established to realize fine-grained authorization and access control in edge computing. Secondly, based on the identity data and behavior log bookkeeping on the chain, the quantification of trust value, trust transmission and update are realized, and the traceability of security events is improved. Finally, based on the improved RAFT consensus algorithm, the multi-party consensus and consistency accounting in the authentication process are realized. Simulation results show that this scheme can meet the requirements of zero trust verification in edge computing environment, and has good efficiency and robustness.

**Keywords:** blockchain; Internet of things; zero trust; edge computing; secret sharing; consensus algorithm

## 1. Introduction

Edge computing is an important form of computing in smart cities [1]. With the rapid development of 5G, chip technology and high-performance intelligent IoT terminals, the computing resources of traditional cloud computing center gradually sink to the sensing layer. In terms of system architecture, the new generation of information technology represented by cloud computing, micro services, big data and AI has significantly changed the IT infrastructure. In the aspect of information processing mode, the wide application of new algorithms such as image-based computing [2], collaborative trajectory [3] and machine learning [4–6] puts forward higher requirements for the security, reliability and effectiveness of information infrastructure [7].

Edge computing unloading the computing power of the cloud center to the user side for data processing, it can alleviate the pressure of the centralized server on multi service concurrency and network bandwidth, and realize flexible and efficient information processing [8]. However, this distributed and open computing structure makes the system have no clear security boundary, resulting in common forms of network attacks, such as physical hijacking, node replication, signal interception, steeling and replaying, man-in-the-middle attack, which are easier to implement and more harmful in the current networking environment [9]. In order to meet these security challenges, it is urgent to study the effective security protection strategy in line with distributed access and dynamic authorization.

Traditional security protection of IT system is mostly the boundary security protection. Different security policies are adopted according to the network location of nodes and resources. This scheme divides the system into different security zones, such as intranet, extranet, VPN, DMZ and so on. Within the security zone, loose security policies are adopted, while outside the security zone, strict security policies are adopted. The security equipment is deployed on the boundary of the security zone and is responsible for the security protection of the security zone. Due to the changes of node scale and access mode in smart city edge computing, the boundary of the security zone is becoming less and less obvious. Because of the lack of awareness and interaction of internal/external security situation, the security protection effect is less ideal.

In view of the above problems of edge computing, people put forward the new concept of zero trust security [10]. The concept of zero trust security breaks the default binding relationship between trust relationship and network location. It is a resource authorization strategy suitable for fuzzy security boundary. It sets dynamic access permissions through user digital identity, and dynamically monitors, real-time evaluates and fine-grained authorizes the resource access process, so that the business trust chain of the edge computing is linked, it realizes stronger dynamic protection ability and higher security credibility.

The principle of zero trust is "never trust, always verify", that is, no matter where in the network, before accessing, all subjects must be authenticated and authorized [11]. Through dynamic permission management and careful resource exposure, the attacked surface of the system can be reduced [12]. The key point of the zero trust architecture is identity centered fine-grained adaptive access control. Therefore, the realization of zero trust mechanism depends on the establishment of an effective identity management system to realize the comprehensive, dynamic and intelligent access control of people, devices, IoT systems and applications in edge computing.

However, for the most common IoT system in smart city edge computing, due to the low processing capacity and battery life of the terminal, it is unable to achieve complex authentication function, and the terminal in the system involves a variety of devices, so it is difficult to choose a

unified attribute as the ID [13]. Therefore, in the process of the implementation of the edge computing system, the concept of zero trust lacks the necessary technical means, and there are little practical zero trust research results for the edge computing.

In order to realize the zero trust mechanism in the edge computing system, we need to solve several critical problems: 1) terminal digital identity; 2) fine-grained authorization, especially according to the behavior portrait of the edge computing terminals; 3) real-time dynamic evaluation of trust value; 4) the reference index of authorization granularity. Blockchain technology is a kind of distributed ledger technology, which realizes the tamper proof property of data through collective bookkeeping. Also, the blockchain has the function of trust value transfer, which provides technical support for digital identity description and trust chain association of edge computing [14].

Based on the blockchain technology, this paper studies the implementation method of zero trust strategy in the edge computing. Based on the proposed terminal identity specification and distributed authentication algorithm on the block chain, we provides a solution for the security protection of edge computing in smart city. The organization of this paper is as follows: Section 2 is the basic principle and existing research review of blockchain and zero trust; section 3 is the architecture of zero trust based on blockchain, as well as the key technology and theoretical research; section 4 is the feasibility of the scheme through simulation experiments.

## 2. Related works

In order to deal with the shortcomings of traditional border security protection strategies in the increasingly expanding access environment, people began to study the security strategy of fuzzy boundary [15]. In 2004, Jericho forum [16] proposed an implicit trust method not limited to the network location. This user driven security strategy does not distinguish the users of internal and external networks, any user accessing a specific resource needs to authenticate and authorize to support the agility requirements of security business.

At the application level, zero trust model establish an end-to-end minimum granularity authorization mechanism between the access subject and the object, in order to improve the implementation difficulty of internal and external attacks, identity fraud and other attacks, and improve the defense response and reaction ability of the system. In 2007, Microsoft anywhere access security technology replaced traditional firewall [17], VPN and other border security facilities, which made employees and users of the company have access to the intranet resources safely in the Internet environment [18]. CSA (Cloud Security Alliance) proposed a zero trust implementation using Software-Defined Perimeter, which only allows access through authentication authorization, so as to ensure dynamic customization of boundary security [19]. In SDP model, sensitive data such as service address and port are hidden in the network, and only visible to authorized users. Before accessing services, controller performs verification and authorization to users and devices, and users only obtain the minimum access point permissions. In 2014, Google implemented a zero trust architecture, called BeyondCorp [20]. By establishing a trusted chain of continuous authentication, Google associated the security relations among users, devices and applications, thus unloading the original security policy on the border to local devices and users. In 2019, NIST released the draft of zero trust architecture, which officially released in 2020 and the concept, architecture, components and scenarios of zero trust are introduced [21].

From the existing implementation mechanism, the basic idea of the zero trust model is no longer

distinguishes between the internal and the external network. The system does not automatically trust any device or person in the internal or external, and verifies any device or person trying to access before authorization. Also, reconstructs the trust basis of access control based on authentication and authorization. Chen et al. [12] researched four key dimensions (i.e. subject, object, behavior and environment) and constructs trustable dynamic access control models, which characterized by security situational awareness, continuous identity authentication, analysis of access behavior, and fine-grained access control. Patil et al. [22] proposed a PoW and PoE based consensus algorithm of blockchain, which satisfy zero trust strategy. In the consensus algorithm, there is an automated mechanism for verification without central authority, and allow data owners to have confidence in the system. Sohaib A. Latif et al. [23] discussed the wide deployment of IoT suffers energy efficiency and security issues and exploits the potential benefits of a blockchain system and integrates it with SDN, which provides research ideas based on blockchain security mechanism.

In present zero trust model, the system needs to verify and protect all sources, restrict and strictly enforce access control, check and record all network traffic logs, in order to achieve borderless security and credibility. However, most of the existing zero trust implementation schemes are based on the traditional data management method based on database, which has the disadvantages of data centralized storage. In the case of large-scale concurrency, there are problems of data consistency and single point failure, it is difficult to synchronize in real time and dynamically update the whole network, and the trust transmission efficiency is low.

In general, the architecture of zero trust horizontally divided into three parts: User, Business agent and resource, and vertically divided into Control Level and Data Level. As shown in Figure 1.

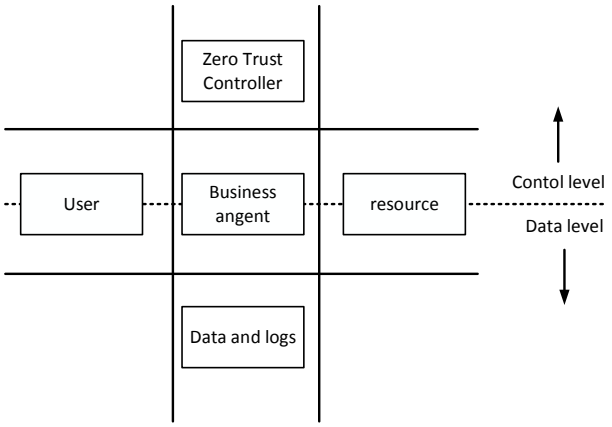


**Figure 1.** Zero trust reference architecture.

Zero trust controller is the core component of the system, which is responsible for initiating authorization and decision-making of access to fuzzy boundary, and carrying out user authentication, permission, trust evaluation, etc. Among them, the evaluation is based on the multi-dimensional [12] user digital identity and credit evaluation system existing in the security library and log set. The business agent, also called zero trust gateway, is responsible for the error free execution of policies, which is a two-way process. One is to collect access information, implement security policies, intercept or release related traffic, the other is to format and store the current processing, and calculate the credit value.

In our opinion, one of the essential differences between zero trust architecture and traditional

architecture is the dynamic association of identity and authority, especially according to the log to analyze the historical behavior, calculate the trust value, and provide the basis for the adjustment of access rights. However, the common zero trust solutions use centralized storage of trust information, which has the disadvantages of single point failure, easy tampering of information, low efficiency of digital identity information collection and use. In view of this, this paper studies the zero trust strategy based on blockchain in the edge computing of smart city. By storing the digital identity information of users and terminals on the chain, the real-time update of the trust chain and the effective transmission of trust information are realized, and the distributed dynamic authorization access of the security system resources of the edge computing agents and terminals are supported.

## 3. Zero trust mechanism

### *3.1. System architecture*

Common edge computing architecture includes perception layer, edge layer, application layer and other components. In operation, the terminal interacts with the application layer through the edge server, carries out access authentication, and obtains resource access rights. Due to the large number of terminals and wide deployment range, it is difficult to guarantee their credibility. The zero trust architecture based on block chain can realize the trusted access and controllable resource access of IoT terminals. The architecture is shown in Figure 2.

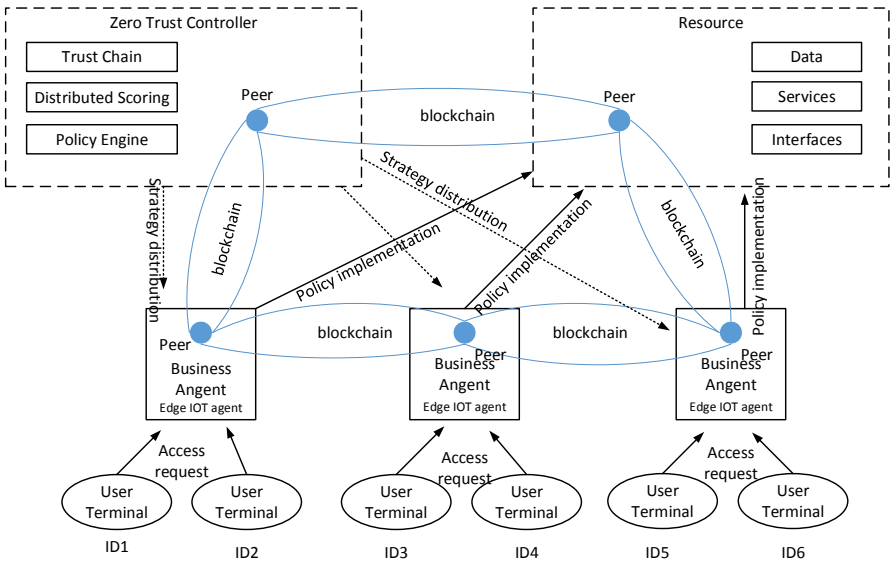


**Figure 2.** System architecture.

The edge server is responsible for managing the digital identity generation, public key authentication and private key update of the terminals under its jurisdiction. When the terminal needs to access the resources, it submits the access request to the edge server. The edge server check whether the user has register and then packages the request and submits it to the blockchain for processing through the intelligent contract. At the same time, for the operation of the blockchain, the smart contract on the zero trust controller is activated. According to the information recorded in the

blockchain ledger, the zero trust controller evaluates the trust value of the request, generates a dynamic access control policy, and sends it to the edge server for execution. The dependent edge servers form a group to run a distributed interactive authentication consensus algorithm, and generate the authentication result of the request event. This event forms a transaction of blockchain and aware to other peers. Then, the edge server starts the corresponding resource access rights. The specific process is shown in Figure 3.

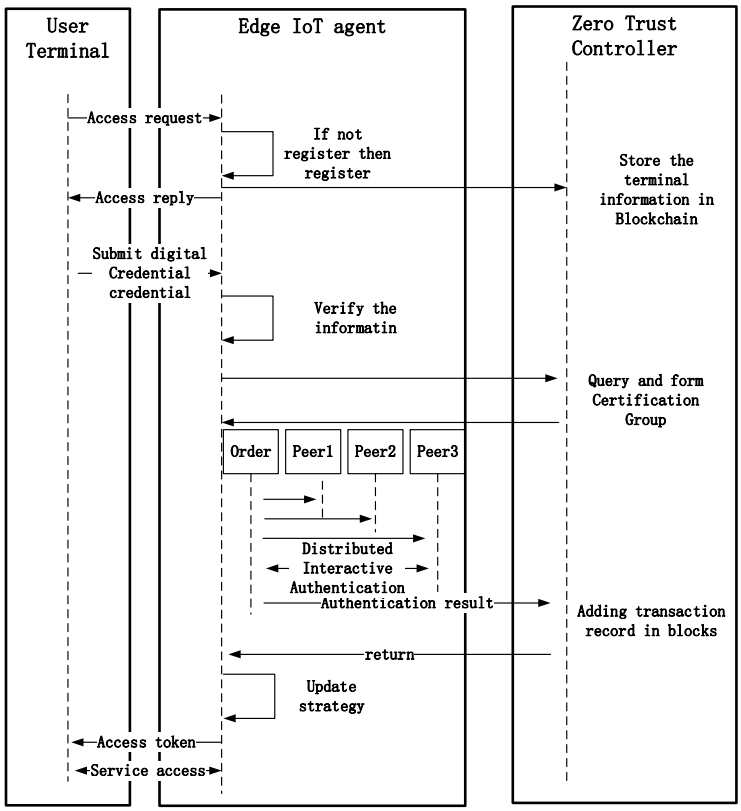


**Figure 3.** Access request processing flow.

In each subsequent access, the edge server intercepts the access of the terminal and the credential verification is triggered. Only the access conforming to the access control policy will be released, otherwise it will be intercepted. The released and intercepted access records are retained to update the data on the trust chain and provide credentials for subsequent access.

### *3.2. Digital identity model*

Digital identity is the key component of zero trust. The zero trust controller calculates the trust value through dynamic query and real-time update of terminal digital identity to provide the basis for authority setting. Because the edge computing terminals are mostly deployed in unattended environment, they are easy to be illegally intruded and controlled, so the identification is particularly important. This research adopts dynamic distributed identity mechanism, uses blockchain distributed ledger to store node identity information and behavior information, forms a network wide consensus and tamper-resistant multi-dimensional identity and authority information portrait, and forms edge

computing terminal trust chain. The zero trust controller dynamically evaluates the terminal according to the trust chain, and finally obtains the zero trust access policy.

### 3.2.1. Data structure

The digital identity based on blockchain structure, which consists of static attributes (S), dynamic attributes (D), evaluation attributes (E) and related smart contract pointers (P). All the attributes are organized by hash tree in block.

Among them, static attributes are fixed attribute information such as device serial number, MAC address, public key, installation time, installation longitude and latitude;

Dynamic attributes include updatable key, authority, authorization level and other variable attribute information of user terminal corresponding to zero trust policy;

The evaluation attribute includes a set of evaluation indicators , including the credit value of the historical access records of the terminal or user, and the parameter data that can be used for trust chain transmission;

Smart contract pointer is used to store smart contracts such as distributed digital identity digital signature, online storage, retrieval, and trust chain transfer. The data structure can be shown as follows:

$DID :=< S >:< D >:< E >:< P >$ where,
$< S >:=< uuID \,||\, MAC \,||\, pub-Key \,||\, T \,||\, (loc-x, loc-y) \,||\, hash >$
$< D >:=< Updatable\ key \,||\, authority \,||\, level >$
$< E >:=< \{indicators : values\} \,||\, \{records : trust\_values\} >$
$< P >:=< \{address \,||\, function\} \,||\, \{parameters\} >$

In order to ensure the identity consistency and tamper-resistant and facilitate query and verification, the digital identity of the terminal is stored in block form, as shown in Figure 4:

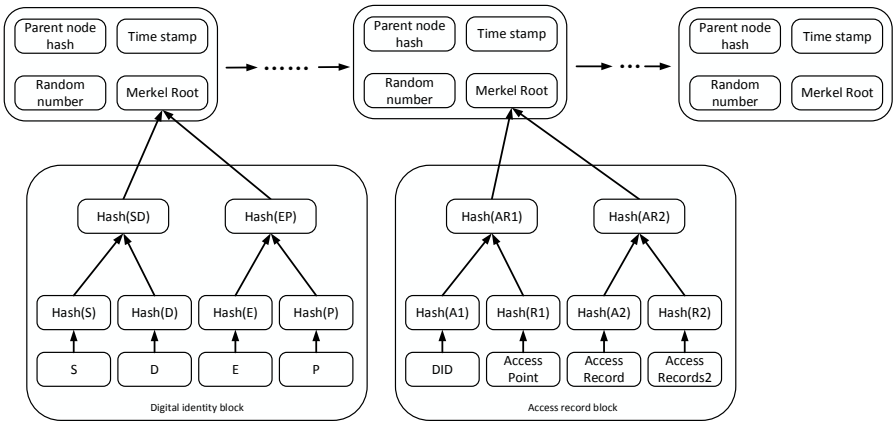


**Figure 4.** Block data structure diagram.

There are two types of blocks in the zero trust system of the edge computing based on block chain, one is the digital identity block (shown in left of Figure 4), the other is the access record block(shown in right of Figure 4). The two blocks exist in the blockchain at the same time and have different functions. That is, the digital identity block mainly records the identity attributes of the user terminal, and the access record block mainly stores the business behavior of the user terminal. In

order to distinguish different types of block nodes and the version of each block, the block type, node version and other information are stored in the random number segment of all blocks, which is calculated as follows:

$$Random\_number = Hash(node\_type \,||\, nonce \,||\, version \,||\, timestamp) \tag{1}$$

In the digital identity block, each block stores the identity attributes of the user terminal, which are organized by the hash process of the binary Merkel tree, that is:

$$\begin{aligned} &MerkelRoot = Hash(SDEP) \\ &= Hash(Hash(SD)Hash(EP)) \\ &= Hash(Hash(S)Hash(D)Hash(E)Hash(P)) \end{aligned} \tag{2}$$

In this way, the digital identity of each user terminal has the characteristics of non-tampering, non-repudiation and traceability. The life cycle of a user's digital identity is defined according to its dynamic attributes. When the dynamic attributes of the terminal change, such as node key update and authority upgrade, the block representing the user's digital identity needs to be updated to generate a new block, so the node's digital identity is updated to adapt to the new access rights. The change of terminal dynamic attributes is dynamically adjusted by the zero trust controller according to the security policy. Its calculation basis and calculation results will depend on the information stored in the block ledger.

In the access record block, the leaf node of binary Merkel tree stores the information contained in each access record, including identity index, access point, access time, access resource number, etc., which is also organized in hash process. It can be seen that the two types of nodes have the same data structure foundation, although their contents and functions are different. In this way, the compatibility and validity of the smart contract can be guaranteed, so that the identity information and access record information are stored in the same account book, which is conducive to the security control of the zero trust controller.

### 3.2.2. Life cycle

The life cycle of digital identity of user terminal includes four processes: creation, use, update and cancellation. It means that the status of each block is recorded in the random digital segment at the head of the block, and can be easily queried and verified. Since digital identity is updated in chronological order, reverse retrieval is adopted to obtain the identity and permissions of the latest version during query. The previous version is only used as access records and audit.

The digital identity creation process of user terminal includes the following steps: firstly, the edge server registers the terminal, packages the initial identity information, key pair, default permission and other attributes of the terminal, and forms the data format that can be processed by the blockchain; Secondly, the consensus algorithm of fixed sorting nodes is used for accounting. The process of blockchain P2P network broadcast also declares the initial access rights of the terminal. At the same time, users can show their digital identity in the process of resource access through the logic in the contract.

According to the access rights information in digital identity, the terminal can show its digital

identity to the verifier. The voucher presented by the user is a temporary voucher generated by the calculation of digital identity and time stamp through single function calculation. On the one hand, the voucher can be submitted to the blockchain system for verification. On the other hand, the verification intelligent contract in the blockchain system can easily complete the verification of the voucher. On the other hand, the voucher is active in a short time, and will not disclose any information of the terminal during the time. The presentation process and basic verification rules of digital identity are as follows:

Step 1: the declarant and verifier determine a random number $r$ as the security parameter of generating the temporary voucher;

Step 2: the declarant forms a temporary certificate use $r$ :

$$certificate = Hash(SDEP \,||\, r) \tag{3}$$

Presents it to the verifier;

Step 3: the verifier calls the intelligent contract to retrieve the latest version of the digital information on the blockchain. Calculate: $verification = Hash(MerkelRoot \,||\, r)$ . If $certificate = verification$ , then, the declarant shows the legal digital identity.

In the zero trust environment, the digital identity of the terminal is dynamically updated, because other attributes in digital identity, except static attributes, change with time. Considering the availability of the system, it is not necessary to trigger the identity update for each attribute change. In the proposed scheme, the update of digital identity can be divided into two cases: regular triggering and event triggering. When the effective time of identity set by zero trust controller arrives, the digital identity of terminal needs to be updated. The intelligent contract is triggered by timer, and data packaging is carried out according to the current attribute state of terminal, forming block and broadcast chain. When events specified by zero trust policy occur, such as terminal access exceeding authority, it needs to be degraded, and intelligent contract will trigger to update the digital identity of users.

If the terminal is scrapped or dismantled, the digital identity of the terminal needs to be revoked, and the revocation process is also processed by the corresponding smart contract. Because the data on the blockchain cannot be deleted, the revocation of the digital identity is performed by chaining a declaration block of digital identity revocation on the sorting node, and its annotation information is stored in the field of the block header. Because the retrieval is performed in reverse order and the revocation declaration block is the latest identity version of the terminal, the system can easily confirm the revocation information of the terminal and withdraw the assigned permissions.

### *3.3. Authentication model*

The zero trust authentication model based on blockchain in the edge computing is shown in Figure 5. As can be seen from the figure, the authentication process includes the process of digital identity formation and credit transmission, all of which are stored in the blockchain ledger. After the terminal's initial digital identity is stored on the blockchain system, with its behavior records in the process of accessing resources, a traceable credit record is formed on the blockchain, and a fine-grained access voucher for specific resources is formed through smart contracts.

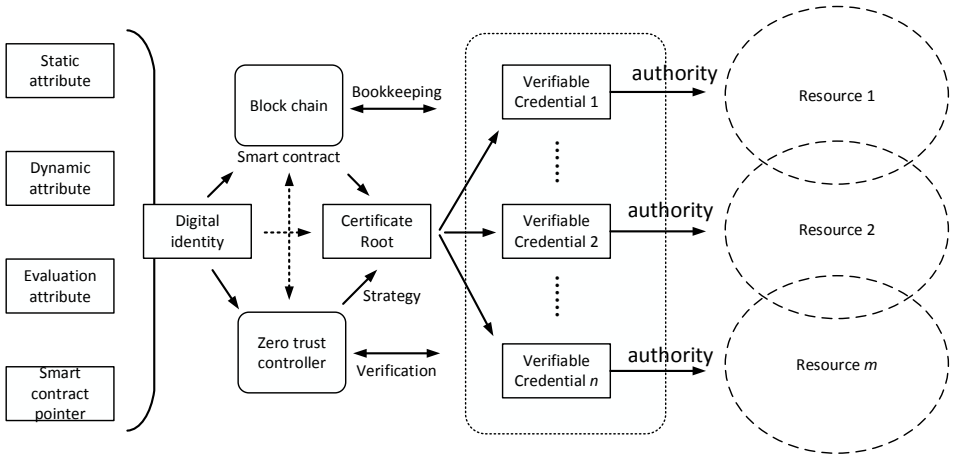


**Figure 5.** Digital identity authentication model.

In the specific implementation process, the digital identity generated according to the terminal attributes is stored in the smart contract chain. The zero trust controller also monitors the creation, use and cancellation of digital identity through a set of smart contracts. In particular, according to the zero trust policy, it is necessary to judge the access behavior of the terminal at any time, such as access point, access resource number, etc., quantify the trust value of the terminal in real time through the trust chain calculation, and call the smart contract to execute the digital identity update policy on demand.

In the edge computing system, according to the digital identity information of the user terminal, it is convenient to generate the credentials of resource access. Assuming that there are resource 1, resource 2 and resource 3 in the system, the zero trust controller obtains the following access credentials by binding the number information of the resource with the digital identity, which are:

$$certificate1 = E(DID, resource1, ap1, timestamp) \tag{4}$$

$$certificate2 = E(DID, resource2, ap2, timestamp) \tag{5}$$

$$certificate3 = E(DID, resource3, ap3, timestamp) \tag{6}$$

where $E(\cdot)$ is the encryption algorithm selected by the zero trust controller. These credentials can access the specified resources within the scope of authorization.

The terminal with access credentials can access the required resources, and it needs to be verified by the zero trust authentication agent before each time it shows its digital identity to access the resources. As the digital identity is stored in the blockchain distributed ledger, the verifier can be easily realized through the smart contract. The specific process is as follows: the authenticator encrypts the digital identity, resource number, access point and access time with the digital identity, traverses the blockchain information through the smart contract, and compares with the query results to obtain the authentication results. Through the event of authentication and successful access, the smart contract will generate an access record block for recording, and the terminal will not be able to deny its access fact and the used credential information.

The trust value can be calculated by authentication record. The terminal has initial permission and

trust value during initialization. When the access content is different from the permission, the trust value will change, that is, if the access is beyond the authority, the trust value will decrease; If the access is authorized, the credit value changes to 0; If you don't use the permission within the authorization time, the credit value decreases with time. If you keep the set usage frequency, the credit value remains unchanged. The above credit value calculation logic is encapsulated in the blockchain system in the form of smart contract and automatically executed and updated to the node's digital identity.

The security characteristic of edge computing is that the local credibility is greater than the global credibility. In order to improve the processing efficiency of the zero trust system, for authentication request of single terminal, the authentication method forms the authentication group through the group with short network distance and conducts distributed authentication.

Suppose the edge computing system consists of $m$ edge servers, which are recorded as $E_1, E_2, \cdots, E_m$. Each edge server manages a terminal group, which are direct connect to the server, denoted by $T_i^{(k)}$. It is assumed that the trust between terminal group and edge server is higher than that between edge server and cloud. Since the results of the authentication process need to be linked for verification, the authentication process is deeply bound with the consensus process. The authentication consensus group is composed of direct connected edge server, neighbor edge agent and nodes with the same network location as the authenticated nodes.

The consensus algorithm with authentication adopts the improved RAFT protocol, in which the leader is only selected from the edge servers. In the election, the direct edge server and the neighbor edge servers rotate in equal proportion.

The specific steps of distributed authentication are as follows:

In the initialization phase, the key management center selects the master key $s$, and distributes the public key and private key pairs $< P_i = Hash(ID_i), D_i = sP_i >$ to each edge server based on IBE algorithm. Where $ID_i$ is the digital identity of $E_i$, which is given by the edge computing system.

Step 1: Create an authentication group with N nodes, an edge IoT agent is selected as the initial leader node by RAFT algorithm, i.e. $E_{l_0}, 1 \le l_0 \le m$, which is also the initiator of distributed authentication.

Step 2: $E_{l_0}$ encrypt the certificate information of the terminal by private key $D_i$, we have:

$$U = En_{D_i}(certificate) = En_{D_i}(Hash(SDEP \,||\, r)) = Hash(SDEP \,||\, r) \oplus Hash(g_{ID}{}^{r}) \tag{7}$$

where, $En_{D_i}$ is the encrypt function of IBE with the private key $D_i$, $g_{ID} = \hat{e}(D_i, sP)$, and P is the generator of additive group (G,+).

Step 3: $E_{l_0}$ uses Lagrange interpolation function to decompose U into w parts, w is the number

of qualified leader nodes in the authentication group, which is generally the edge servers with sufficient computing resources. The decomposition method is as follows:

(i) Select the coefficient vector of w-dimensional interpolation polynomial $\{a_j \mid a_j \in G^*; j=1,2,\cdots,w-1; a_{w-1} \neq 0, 1 \leq w \leq N\}$, construct the interpolation polynomial:

$$F(x) = U + \sum_{j=1}^{w-1} a_j x^j = Hash(SDEP \| r) \oplus Hash(g_{ID}{}^r) + \sum_{j=1}^{w-1} a_j x^j \tag{8}$$

(ii) Calculate the share of each node in the authentication group:

$$F(i) = U + \sum_{j=1}^{w-1} a_j i^j \ , \ 1 \leq i \leq N; \tag{9}$$

The initial leader broadcasts $F(i)$ through heartbeat information, and the broadcast information is encrypted by the public key of each member (in the consensus authentication group), so that each node can only open its own key share.

Step 4: Distributed authentication stage, the authentication group implements the distributed authentication consensus based on raft for the authentication requests of nodes. In raft consensus algorithm, the status of each node can be leader, candidate and follower, and $E_{l_0}$ in initial state. In distributed validation consensus algorithm, there are the following stages:

(i) The leader election stage

The first leader $E_{l_0}$ completes the shadow key distribution during his term of office, and then exits the leader state by stopping sending heartbeat information. When other nodes except $E_{l_0}$ do not receive $E_{l_0}$ heartbeat information, they change from following to candidate. This process is generated by competition. Assuming that the current candidate is $E_{l_x}$, $E_{l_x}$ initiates a vote and requires other nodes to submit the distributed authentication results of the admission request node. If a node agrees to the authentication request, it sends the secret share information encrypted with $E_{l_x}$'s public key to the candidate.

(ii) Log replication phase

When the candidate $E_{l_x}$ obtains more than the threshold value of *w* key shares, it decrypts the encrypted information with its own private key, and becomes a new leader with one term of accounting authority. Other nodes become followers, and the system enters the log replication stage. In this stage, $E_{l_x}$ calculates the encrypted request data by Lagrange interpolation:

$$U = \sum_{j=1}^{w} F(i) \prod_{1<l<w, l \neq j} \frac{x_l}{x_l - x_j} \tag{10}$$

The above results are verified by smart contract. After passing the verification, the access information is packaged to form a new block and account, and the account book is broadcast to all nodes.

## 4. Simulation analysis

In order to study the feasibility of the proposed scheme, we build the edge computing zero trust simulation system based on the alliance blockchain. The system environment includes a cloud service, a zero trust controller and four edge servers. Among them, the cloud service is deployed in the cloud server, the zero trust controller and the edge servers are deployed in five servers running IoT business and blockchain node programs. There are 12 user terminals. The simulation topology is shown in Figure 6.

The server configured Intel i7-7700HQ CPU@2.80GHz, with 16GB DDR4 memory, and 512GB SSD hard disk, the operating system is CentOS 7. The IoT terminals are running by raspberry pies, which are 3B version and configured with BCM2837B0 SOC, which CPU integrates 4-core ARM Cortex-A53 64-bit @1.4 GHz and 1 GB LPDDR2 SDRAM. The system configuration refers to the software and hardware configuration of the mainstream cloud edge IoT system in the smart city in terms of system resources and hardware performance, so it is representative.

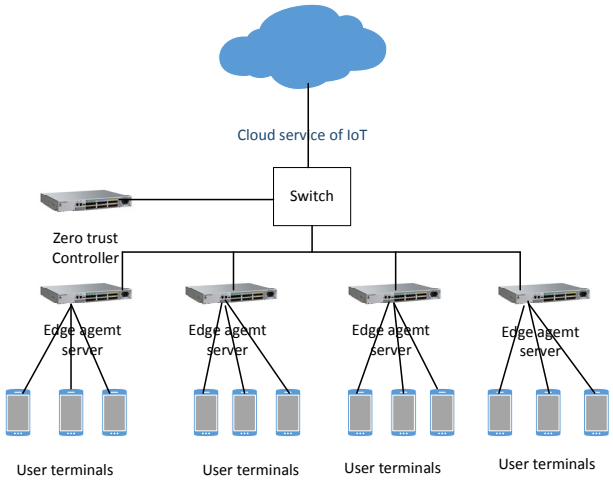


**Figure 6.** Simulation topology.

The digital identity of the terminal is the basis for the controller to assign access rights in the zero trust environment. In this scheme, the digital identities of all user terminals are stored in the form of blockchain ledger, which has the functions of tamper proof, traceability, trusted exchange, and privacy protection. The digital identity of terminal is updated at any time with the change of zero trust policy and terminal access behavior, so its initialization process and update process are the process of blockchain data on the chain, which correspond to the generation of new blocks.

Figure 7 shows the delay curve of digital identity generation and update in the experimental environment. The experiment counts the delay required for 0–100 digital identities generation and update. In the case of concurrency of the same order of magnitude, this scheme has advantages over the existing scheme.

It should be noted that a terminal may issue multiple requests, and the value recorded in the simulation is the number of requests, not the number of terminals. As a comparative analysis, we also make statistics of the traditional IoT system using relational database to store user data, which denoted

as “non DID shcme” in Figure 7. At the same time, we also compare and analyze Guo’s scheme [9] when peer number is 10. It can be seen from the simulation results that the delay increases with the increase of the number of requests. When the number of requests increases from 20 to 100, the delay increases from 1000 to 11500 ms, but it is still in the acceptable range for the Internet of things systems in smart city. From the comparison scheme, the scheme based on relational database to store identity information has some advantages in delay, but this non digital identity scheme does not have the advantages of distributed consensus and tamper proof of blockchain schemes. Compared with Guo’s scheme, when the number of concurrent requests is less than 80, the proposed scheme has obvious advantages, but when the number of concurrent requests continues to increase, the delay of Guo’s scheme tends to increase linearly, and the delay increases due to more zero trust processing in the proposed scheme.

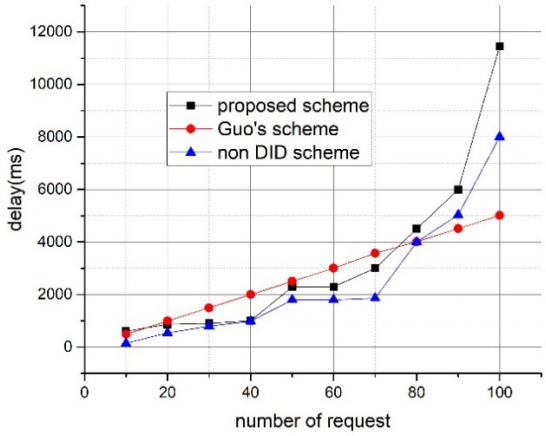


**Figure 7.** Delay curve of digital identity generation and update.

Compared with the traditional system, the frequency of authentication process in zero trust system increases greatly, which affects the overall time performance of the system. For the blockchain based system studied in this paper, the time cost of authentication includes not only the latency caused by the calculation of the algorithm itself, but also the cost of searching the digital identity information stored in the blockchain ledger. During the simulation experiment, we counted the time cost of 100 verification requests, and the results are shown in Figure 8. As a comparison scheme, we remove the mechanism of confirmation at any time in zero trust in the proposed scheme, and take the last successful authentication as the reference basis for resource authorization.

It can be seen from the figure that the time cost of digital authentication is on the rise. When the number of concurrency is less than 20 times, the time cost can be ignored. When the number of concurrency exceeds 50, the delay increases greatly. This is because the increase in the number of concurrency leads to frequent block chain ledger queries and the increase in hash operations per unit time. In the comparison scheme, when the number of concurrency is less than 70, the delay of authentication request is not much different from the proposed zero trust scheme, which belongs to the same order of magnitude; When the number of concurrency exceeds 70, the system delay decreases significantly due to the reduction of authentication complexity. To sum up, in absolute terms, the increase in the number of concurrency leads to the increase in block chain ledger queries, the system delay is still in the acceptable range, which has little impact on the system availability.

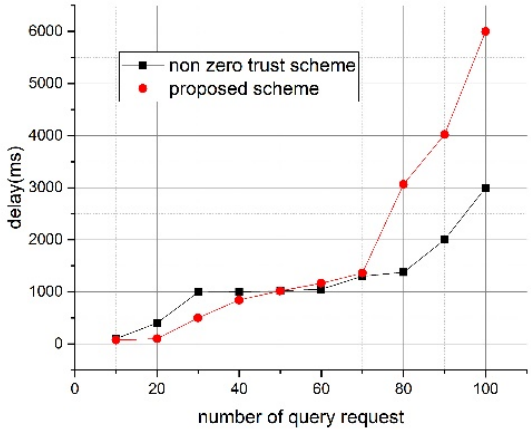


**Figure 8.** Delay curve of digital identity authentication.

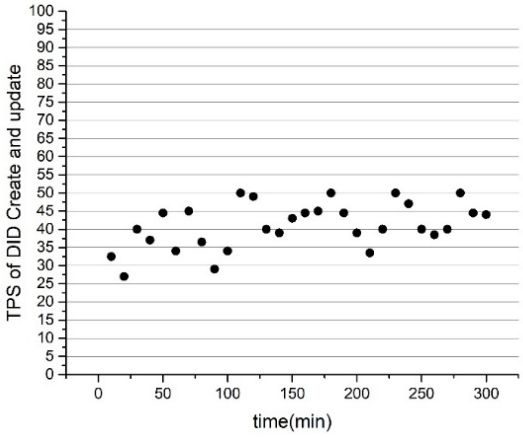


**Figure 9.** TPS curve of digital identity generation and update.

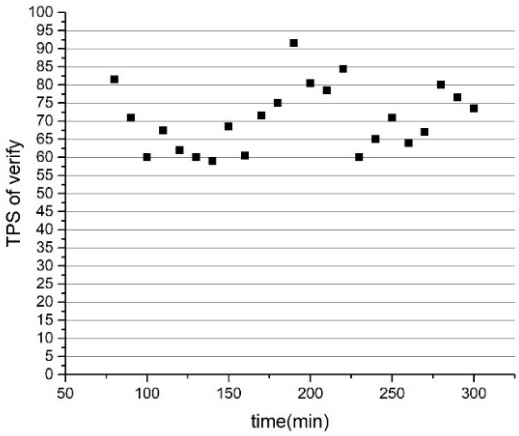


**Figure 10.** TPS curve in the process of zero trust verification.

TPS (transaction per second) is defined as the traffic that blockchain can process per second, and it is an important index to evaluate the performance of blockchain system. In the simulation, we adopt

a 300 minutes period of stress test strategy, through saturated service request to verify the throughput of the system. Figures 9 and 10 are TPS values measured at each sampling point during the test time, which generate updates and zero trust verification for digital identity respectively. The results show that the TPS value of the system is stable, with the mean value of about 40. TPS measurement in this simulation process is not only the performance of blockchain, but also the processing of cryptography algorithm, especially the verification process. It is the whole process of terminal authentication from initiation to authentication group confirmation, chain storage and interactive verification. Therefore, although the number of TPS is lower than that of pure blockchain platform, it is fully qualified for the authentication requirements of the traditional Internet of things zero trust system.

During the 300 minutes' stress test, we also measured the consumption of basic resources of the system. Among them, CPU and memory usage overhead data is shown in Figure 11. During the simulation period, we sampled the system resource occupation. The feasibility study shows that the load of system basic resources such as CPU and memory is relatively stable. The average CPU occupation is about 65%, and the memory overhead is about 50%. It shows that the system runs stably.

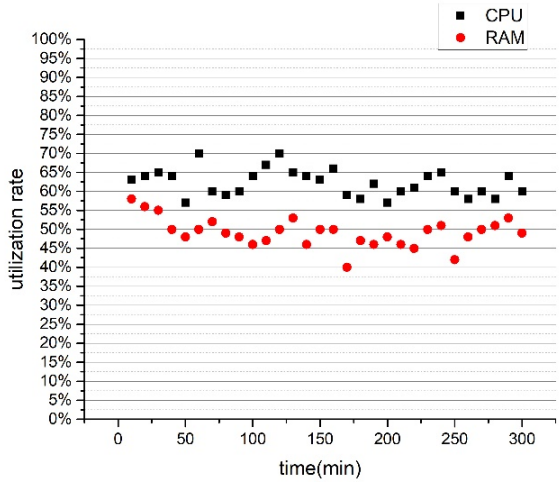


**Figure 11.** System performance curve.

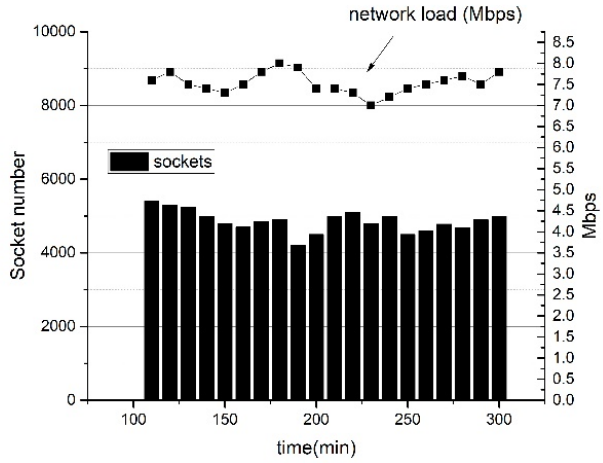


**Figure 12.** Network performance curve.

For P2P network performance, during 300 minutes of test, the number of blockchain network connections and network throughput are shown in Figure 12. From the simulation results, the data packets of the system are stable at 4300 sockets, and the network throughput is 7.5 Mbps, indicating that the network is running well.

In order to verify the impact of different modules in the proposed scheme on the system performance, we experimentally study the performance comparison curves of the complete scheme and the two simplified schemes. Simplification scheme 1, which called the basic block data structure, simplifies the data structure of the block, and only store transaction information without classified management. Simplified scheme 2 named computing offload scheme, which offloads the authentication request of the terminal to the edge side, and only validates the authentication edge IoT agent, that is, the terminal directly connected to the legitimate edge IoT agent is regarded as a trusted terminal. The comparative experimental results are shown in Figure 13.

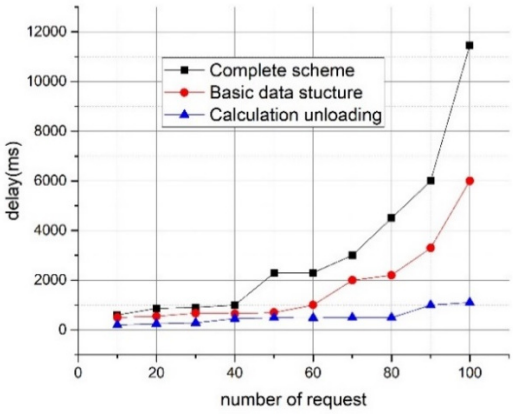


**Figure 13.** Experimental curve after changing scheme parameters.

It can be seen that the time cost of the scheme can be reduced to a certain extent through two simplified schemes. Macroscopically, the performance of the calculation unloading scheme is better than that of the basic data structure scheme, and the delay change curve is smooth, while the performance of the basic data structure scheme is better than that of the complete scheme. In terms of average delay, there is no significant difference in delay in 40 concurrent cases. However, in the case of 0–100 concurrent requests, the average delay of the basic data structure can be reduced by 40%. The simplified scheme based on computational offload further optimizes the average delay under the same concurrency, which is 59% lower than that of the basic block scheme. Therefore, in the actual implementation of the scheme, if the system is highly trusted, the scheme of simplifying the data structure can be adopted; If there are many edge nodes, consider unloading more computing resources to the edge side under the condition of meeting the security level.

The number of terminal nodes is also an important factor affecting the system performance. In order to verify the scalability of the system, we analyze the system performance under different number of terminal nodes through experiments. In the proposed scheme, the edge agent server, zero trust controller and system resources are all used as peer nodes of the blockchain system, and the user terminals are directly connected to the corresponding edge agent server. There is only one resource peer node in the experimental setting, and 4, 8 and 16 peer nodes are set in the edge proxy server

respectively (that is, the total number of peer nodes is 6, 10 and 18). Each edge proxy server can connect 3, 4 and 5 terminals. The measured system delay is shown in Figure 14.

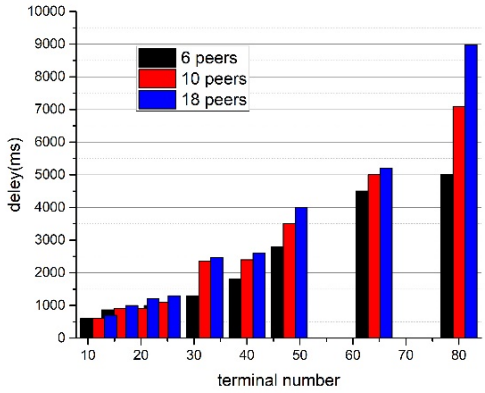


**Figure 14.** Authentication latency with different number of terminals and peers.

**Table 1.** Performance comparison of different schemes.

| Scheme | System parameter | Network performance | Average latency(ms) |
|---|---|---|---|
| LSCCOA [8] | CPU: 300 MHz<br>Network: LTE-A + fiber Wi-Fi network<br>Terminal number: 60–1200 | Throughput: 1166.2 bps | 39592 |
| PBT [24] | CPU: 2.8 GHz<br>Network: P2P network<br>Terminal number: 0–1200 | Network load: 320 Kb | 6000 |
| Literature [25] | CPU: 3.2 GHz<br>Network: P2P network<br>Terminal number: 0–100 | Network load: 109 Kb | 34000 |
| Literature [26] | Network: Fog Computing network + P2P | Network load: 2080 b | 245 |
| The proposed scheme | CPU: 1.4 GHz<br>Network: P2P + Wi-Fi network<br>Terminal number: 0–100 | Throughput: 7.5 Mbps | 3000 |

It can be seen from the experimental results that with the increase of terminal nodes, the system delay tends to increase, and the increase range is close to that of concurrent request experiment. This is because each terminal has a unique digital identity, and there is no great difference between concurrent request and concurrent terminal. Under the same node size, the more peers, the greater the system delay. This is because the role of different peers is similar to that of authentication domain. The more peers, the higher the system overhead required for mutual authentication, but this setting can reduce the coupling degree of smart city edge computing system and improve the scalability and compatibility of the system.

The performance comparison between the proposed scheme and the existing edge computing scheme under the same experimental conditions is analyzed below. The comparison results are shown in Table 1.

Compared with the existing schemes, the proposed scheme has certain advantages in network performance and computing performance. Among them, LSCCOA scheme [8] is an edge computing resource unloading scheme, which can optimize the edge side and terminal side resources through resource unloading technology; PBT scheme [24], literature [25] scheme and literature [26] scheme are all blockchain based schemes. The network environment adopted is P2P network. Since zero trust mechanism is not adopted, literature [26] scheme has the best latency, which is 245 ms. The proposed scheme fully considers the optimization of blockchain nodes and authentication process, and has the optimal network throughput on the premise of ensuring the average delay.

## 5. Conclusions

With the development of information and communication technologies such as 5G and Internet of things, the access range of edge computing in smart city is further increased, and the types and functions of intelligent terminals are becoming more and more complex. The traditional security protection means based on network boundary are facing greater challenges in the new application mode and security environment. The zero trust scheme based on the user's digital identity can easily tracking, research and judgment of terminal behavior, which can well deal with the security problems in the fuzzy security boundary. Through fine-grained and minimized resource access authorization, the security performance of edge computing is improved. Based on the block chain distributed ledger and consensus algorithm, this paper proposes an effective zero trust authentication scheme suitable for edge computing. Through the management of the whole life cycle of generation, update and verification of distributed digital identity, combined with the improved RAFT consensus authentication protocol, this paper realizes the zero trust control of real-time verification and dynamic authorization of terminal. Simulation results show that the proposed scheme has good performance. In the further work, the scheme optimization for specific hardware will be studied to further improve the availability of the system.

## Acknowledgments

This research was funded by the Philosophy and Social Science Foundation of the Jiangsu Higher Education Institutions of China "Research on Blockchain-based Intelligent Credit Information System and its Privacy Preservation Mechanism" (Grants No. 2021SJA0448), and the Natural Science Foundation of Jiangsu Province (Grants No. BK20210928).

## Conflict of interests

The authors declare no conflicts of interest in this article.

## References

1. R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: a survey, some research issues and challenges, *IEEE Commun. Surv. Tutorials,* **21** (2019), 1508–1532. http://doi.org/10.1109/COMST.2019.2894727

2. T. Ma, H. Wang, L. Zhang, Y. Tian, N. Al-Nabhan, Graph classification based on structural features of significant nodes and spatial convolutional neural networks, *Neurocomputing,* **423** (2021), 639–650. https://doi.org/10.1016/j.neucom.2020.10.060
3. Y. Tian, B. Song, M. Murad, N. Al-Nabhan, Trustworthy collaborative trajectory scheme for continuous LBS, *Int. J. Sens. Networks,* **38** (2022), 58–69. http://doi.org/10.1504/IJSNET.2022.120275
4. L. Fu, Z. Li, Q. Ye, H. Yin, Q. Liu, X. Chen, et al., Learning robust discriminant subspace based on joint L2,p- and L2,s-norm distance metrics, *IEEE Trans. Neural Networks Learn. Syst.,* **33** (2022), 130–144. https://doi.org/10.1109/TNNLS.2020.3027588
5. Q. Ye, P. Huang, Z. Zhang, Y. Zheng, L. Fu, W. Yang, Multiview learning with robust double-sided twin SVM, *IEEE Trans. Cybern.,* **2021** (2021). https://doi.org/10.1109/TCYB.2021.3088519
6. Q. Ye, Z. Li, L. Fu, Z. Zhang, W. Yang, G. Yang, Nonpeaked discriminant analysis for data representation, *IEEE Trans. Neural Networks Learn. Syst.,* **30** (2019), 3818–3832. https://doi.org/10.1109/TNNLS.2019.2944869
7. Z. Tong, F. Ye, M. Yan, H. Liu, S. Basodi, A survey on algorithms for intelligent computing and smart city applications, *Big Data Mining Anal.,* **4** (2021), 155–172. https://doi.org/10.26599/BDMA.2020.9020029
8. J. H. Anajemba, T. Yue, C. Iwendi, M. Alenezi, M. Mittal, Optimal cooperative offloading scheme for energy efficient multi-access edge computation, *IEEE Access,* **8** (2020), 53931–53941. https://doi.org/10.1109/ACCESS.2020.2980196
9. S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: a distributed and trusted authentication system, *IEEE Trans. Ind. Inf.,* **16** (2020), 1972–1983. https://doi.org/10.1109/TII.2019.2938001
10. P. Zhang, C. Tian, T. Shang, L. Liu, L. Li, W. Wang, et al., Dynamic access control technology based on zero-trust light verification network model, in *2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, (2021), 712–715. https://doi.org/10.1109/CISCE52179.2021.9445896
11. A. Wylde, Zero trust: Never trust, always verify, in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, (2021), 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478244
12. B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, et al., A security awareness and protection system for 5G smart healthcare based on zero-trust architecture, *IEEE Int. Things J.,* 8 (2021), 10248–10263. https://doi.org/10.1109/JIOT.2020.3041042
13. D. Li, X. Gao, A blockchain based terminal security of IoT, in *ICBDS 2019, CCIS 1210,* (2019), 445–454. https://doi.org/10.1007/978-981-15-7530-3_34
14. J. Zhang, Z. Wang, L. Shang, D. Lu, J. Ma, BTNC: A blockchain based trusted network connection protocol in IoT, *J. Parallel Distrib. Comput.,* **143** (2020), 1–16. https://doi.org/10.1016/j.jpdc.2020.04.004
15. S. Mehraj, M. T. Banday, Establishing a zero trust strategy in cloud computing environment, in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, (2020), 1–6. https://doi.org/10.1109/ICCCI48352.2020.9104214
16. C. Saran, Cliff, Jericho Forum presents strategy for secure access for businesses, *Comput. Wkly.,* **3** (2004), 16.

17. B. Gates, *Enabling secure anywhere access in a connected world*, 2007. Available from: https://www.metamuse.net/2007/02/bill-gates-enabling-secure-anywhere.html.
18. J. Morello, Secure access anywhere, *Technet Mag.,* 2007.
19. *Software defined perimeter (SDP) and Zero Trust*, 2020. Available from: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/.
20. R. Ward, B. Beyer, Beyondcorp: a new approach to enterprise security, *Login Mag. USENIX SAGE,* **39** (2014), 6–11.
21. NIST, *Zero trust architecture: draft NIST SP 800-207 available for comment*, 2019. Available from: https://www.nist.gov/news-events/news/2019/09/zero-trust-architecture-draft-nist-sp-800-207-available-comment.
22. A. P. Patil, G. Karkal, J. Wadhwa, M. Sawood, K. D. Reddy, Design and implementation of a consensus algorithm to build zero trust model, in *2020 IEEE 17th India Council International Conference (INDICON)*, (2020), 1–5. https://doi.org/10.1109/INDICON49873.2020.9342207
23. S. A. Latif, F. Wen, C. Iwendi, L. Wang, S. Mohsin, Z.Han, et al., AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems, *Comput. Commun.,* **181** (2022), 274–283. https://doi.org/10.1016/j.comcom.2021.09.029
24. Y. Jia, S. Sun, Y. Zhang, Q. Zhang, L. Ding, Z. Liu, et al., PBT: a new privacy-preserving payment protocol for blockchain transactions, *IEEE Trans. Dependable Sec. Comput,* **19** (2022), 647–662. https://doi.org/10.1109/TDSC.2020.2998682
25. M. A. Azad, S. Bag, F. Hao, A. Shalaginov, Decentralized self-enforcing trust management system for social Internet of Things, *IEEE Int. Things J.,* **7** (2020), 2690–2703. https://doi.org/10.1109/JIOT.2019.2962282
26. D. Ngabo, D. Wang, C. Iwendi, J. H. Anajemba, L. A. Ajao, C. Biamba, Blockchain-based security mechanism for the medical data at fog computing architecture of Internet of Things, *Electronics,* **10** (2021), 2110. https://doi.org/10.3390/electronics10172110


AIMS Press

©2022 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)