Trusted Access Mechanism of Field Device in Industrial Edge Computing Environment

Tao Yu
China-Korea Belt and Road Joint Laboratory on Industrial Internet of Things
Chongqing University of Posts and Telecommunications
Chongqing, China
yutaofeng_1218@163.com

Min Wei*
China-Korea Belt and Road Joint Laboratory on Industrial Internet of Things
Chongqing University of Posts and Telecommunications
Chongqing, China
weimin@cqupt.edu.cn

Feng Xiao
China-Korea Belt and Road Joint Laboratory on Industrial Internet of Things
Chongqing University of Posts and Telecommunications
Chongqing, China
13438020786@163.com

Haoyue Yang
China-Korea Belt and Road Joint Laboratory on Industrial Internet of Things
Chongqing University of Posts and Telecommunications
Chongqing, China
yanghyalicea@163.com

Abstract—With the increasing access of field devices into industrial networks, establishing a trusted access mechanism has become a critical precondition for the deployment of industrial networks. In order to ensure the trustworthiness of field devices in industrial edge computing environments, the reputation mechanism should be solved, which can be achieved through the trusted access mechanism in proposed. The mechanism outlined in this paper incorporates two methods. The first method involves field device authentication based on reputation value, and the second method focuses on trust evaluation based on comprehensive evaluation. Distinguished from the traditional PBFT and RBFT where all nodes participate in the consensus, high-scoring nodes are selected to participate in the consensus based on their reputation values, dynamically updating the reputation values. A test platform has been developed for validating this mechanism, with results indicating that the time of authentication and consensus have been reduced, the detection rate of the proposed trust evaluation mechanism has been improved, confirming the stable feasibility and good reliability of the proposed trusted access mechanism.

Keywords—Edge Computing, Security, Authentication, Trust Evaluation

I. INTRODUCTION

With the help of the computing and storage characteristics of Edge Computing (EC), industrial networks can provide closer services to industrial field device on the edge side, which slowing down the data and computational load in industrial networks, and improving real-time response capability[1]. However, edge computing allows a large number of field device to access the industrial network, resulting in a large number of attacks moving from the cloud layer to the industrial field layer, and bringing more and more serious security challenges to the industrial network[2]. Meanwhile, in the context of open networks, the authentication mechanism among multiple entities has become more prominent. The security of industrial edge computing networks will be threaten seriously by malicious field device if there is a lack of authentication at the edge side[3-5]. Therefore, ensuring the trusted access of field device in the industrial edge computing environment is an urgent problem to be solved in the current industrial edge computing security.

In recent years, many researchers have proposed various authentication methods for different services and application scenarios of the IoT. Sarvabhatla[6] proposed a device with fingerprint recognition capability to expand the application scenarios of wireless sensors in industrial networks. Tsai[7] has proposed a new anonymous authentication method scheme in a distributed mobile cloud service environment. Ben[8] proposed a new computational anonymous security authentication scheme based on edge/fog which improves the security and privacy protection capabilities. References [7-8] both use bilinear pairing, causing significant time overhead for the entire mechanism. For the difficulty of computational overhead, Kaur[9] proposed a lightweight and privacy protected virtual authentication protocol for mobile edge computing environment.

Behavior and identity trust are important research topics in the trusted evaluation technology under the edge computing environment[10]. In response to the problems of long response time and low malicious detection rate of existing trust computing schemes in dynamic edge environments, Kong[11] proposed a task offloading strategy based on a multi feedback trust mechanism framework. Monir[12] proposed a trust evaluation scheme for service providers to determine service level agreements, but it can not meet the lightweight computing requirements of resource constrained device. Li[13] proposed a non-redundant indirect trust search algorithm based on a cross domain trust model. Ma[14] has built a system with self configurable functions based on the open source features of blockchain, which providing stronger security protection capabilities for trusted data management systems.

To sum up, in recent years, scholars have combined blockchain and cryptography to study the authentication mechanism with distributed, efficient and traceable characteristics to meet the needs of industrial edge computing scenarios for authentication[15]. Moreover, the research found that the trust evaluation mechanism can evaluate the security of itself and the system access equipment through the analysis of data and behavior in the system.Therefore, this paper proposed a trusted access mechanism for field device in industrial edge computing environment. On the basis of the trusted access framework design of field device in the edge environment, the legitimacy authentication and trust evaluation of Edge equipment are realized by combining the consortium blockchain, effectively avoiding the disadvantages of centralized authentication and improving the reliability of authentication results. The research arrangement is as follows. The second part introduces the system framework and proposes a trusted access mechanism for field device in industrial EC environment.In the third section, a test platform is developed to verify the proposed method, and the research results are analyzed and discussed. Finally, summarize the paper.

II. FRAMEWORK AND METHODS

A. Framework

On the basis of the industrial edge computing reference framework, a trusted access framework for field devices is proposed in this paper , which consists of the industrial cloud platform layer, the edge layer and the field layer from top to bottom, as shown in Fig.1.

(1) The industrial cloud platform layer includes Industrial Cloud Server (ICS), which provides information computing and storage services for edge layer consortium blockchain nodes and field layer device.

(2) As an intermediate layer, the edge layer not only has data transmission capabilities, but also has data processing capabilities, including edge servers, edge agents, edge gateways, and switches.

- Edge Server (ES) is a device with computing and storage capabilities. It installs a consortium blockchain client in the edge server to form a consortium chain node, which maps the consortium chain as shown in Figure 1. The consortium chain is a logical structure of edge nodes and there are no connections to other devices in the proposed architecture.
- Edge Agent (EA) is a device with communication, data storage, computation, and detection functions.
- Edge Gateway (EG) is responsible for generating transaction information for authentication of terminal device and implementing network communication.
- Switch (S) is mainly responsible for extending network interfaces in the framework to facilitate communication between edge servers, edge agents, and edge gateways.

(3) The field layer includes field device and routing nodes.

- Field Device (FD) completes the perception of the environment and collecting data.
- Route (R) completes data forwarding, routing path selection, and data integrity construction in the recommendation trust stage in the field layer.

B. Field device authentication method based on reputation value

1) **Symbol description**

The symbols used in the terminal authentication mechanism based on the reputation are shown in Table I.

2) **Initialization**

Step 1: System initialization

P_{EG} is generated by the edge gateway based on B_{EG}, S_{EG} is generated by the random generation function and P_{EG}. Meanwhile, the public-private key pairs of field device is generated by the edge gateway based on $NodeID_{FD}$ and B_{RD}. Then the consortium chain client within the edge server is installed, ES_i uses asymmetric encryption algorithm to obtain a unique session key pair.

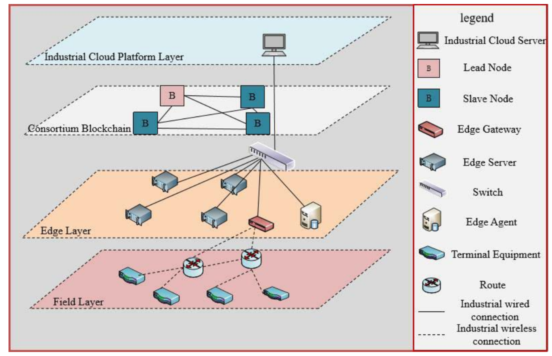

Fig. 1. Trusted access framework for field device

TABLE I. SYMBOLS USED IN THE AUTHENTICATION MECHANISM

Name	Description
EG	Edge Gateway
FD	Field Device
R	Route
ES	Edge Server
B_{EG}	The device ID of Edge Gateway
P_{EG}	The Public Key of Edge Gateway
S_{EG}	The Private Key of Edge Gateway
P_{FD}	The Public Key of Field Device
S_{FD}	The Private Key of Field device
P_R	The Public Key of Route
S_R	The Private Key of Route
ES_i	i-th Edge Server
P_{ES_i}	The Public Key of the i-th Edge Server
S_{ES_i}	The Private Key of the i-th Edge Server
‖	Link symbols
E( )	Elliptic curve cryptography
ES( )	Elliptic curve digital Signature algorithm
Hash( )	Hash function operation
E'( )	Asymmetric encryption algorithm
G	Basic point
B_{EG}	Equipment identification of edge gateway
$NodeID_{FD}$	Field device node identification
Z	Total number of nodes in consortium blockchain

Step 2: Selecting consensus nodes, lead nodes, and slave nodes based on reputation value mechanism

Within Δt before the start of each round of registration information on the chain, the consensus node will be selected based on the reputation value of the federated chain node and a random verifiable function [16-17] (VRF). ES_i generates a random number $rand_i$ and broadcast it, where $i \in [1, Z]$.Meanwhile, $p = r_l/R_a$ is used in this paper to determine the threshold for consensus selection, r_l represents the reputation value of the alliance chain node itself, R_a represents the reputation value of all alliance chain nodes. When $result_i = \mathrm{VRF\_Hash}(S_{ES_i} \parallel rand_i)$ meets $\frac{result_i}{2^{len(result_i)}} \in [0,1] \leq p$, ES_i is qualified to become a consensus node, and len($result_i$) is the length of $result_i$.

After completing the selection of consensus nodes, the new LN will be selected by the Lead Node (LN) in the previous cycle, which with the highest reputation value based on the behavior information in Table II, and the last N nodes will be the new Slave Nodes (SN).

Step 3: Initialization phase of registration request message generated by field device

S_{FD} is used to asymmetric encrypt ($P_{FD} \parallel NodeID_{FD}$) by field device, then $A_0 = \mathrm{E'}_{S_{LN}}(P_{FD} \parallel NodeID_{FD})$ is obtained. The identity registration information (ms) of the field device is generated: $ms = (P_{FD}, NodeID_{FD}, t_b, A_0)$, where t_b is the current timestamp. FD encrypts ms by using elliptic curve cryptography to obtain registration request message $req = \mathrm{E}_{\mathrm{P_{EG}}}(P_{FD} \parallel NodeID_{FD} \parallel t_b \parallel A_0)$ then FD sends the req and current timestamp T_r to EG.

TABLE II. NODE CREDIT VALUE AND BEHAVIOR INFORMATION

Attribute	Identification
Lead Node	LN
Slave Node	SN
Lead Node reputation value	r_{LN}
Slave node reputation value list	$r_{SN} = \{r_{SN_1}, r_{SN_2}, \ldots r_{SN_N}\}$
The times of the lead node has uploaded the identity registration information	S
The times of the identity registration information of the main node has not been linked	F
The times of consensus failures during the uplink phase of slave node identity registration information	$G_f = \{g_1, g_2, \ldots g_N\}$
The times of duplicate consensus reached from slave node sending	$G_{e_j} = \{g_{e_1}, g_{e_2}, \ldots g_{e_N}\}$
The total number of consensus during the uplink phase of identity registration information	$Link$

Step 4: Edge gateway verification registration request message and lead node verification registration transaction stage

After receiving the req, EG checks whether req has expired, then verify whether the ms' obtained from deciphering the req is equal to the ms. If the verification has passed, EG will calculate $h = \mathrm{Hash}(\mathrm{P_{FD}} \parallel \mathrm{NodeID_{FD}} \parallel \mathrm{t_b} \parallel \mathrm{A_0})$ to obtain the signature $sig_{S_{EG}}(h)$, a registration transaction will be generated, then EG sent it to LN, where $trans_{EG} = (P_{FD}, NodeID_{FD}, t_b, A_0, sig_{S_{EG}}(h))$ .After receiving $trans_{EG}$, LN checks whether it is within the validity period. If it passed, then verifies whether its sender is EG. If the verification passed, LN will place ($NodeID_{FD}, t_b, A_0$) in $trans_{EG}$ into the trading pool; if not passed, registration failed.

Step 5: Transaction information generation and verification stage of field device

LN obtains （$NodeID_{FD}, t_b, A_0$） from the trading pool and generates transaction information $trans_{LN} = (\mathrm{E}_{P_{RN'}}, T\_tx)$, then broadcasts $trans_{LN}$ to other SNs, where $\mathrm{E}_{P_{RN'}}(NodeID_{FD}, t_b, A_0, \mathrm{E'}_{S_{LN}}(h_3))$ is denoted as $\mathrm{E}_{P_{RN'}}$, $h_3 = Hash(NodeID_{FD} \parallel t_b \parallel A_0)$, T_tx is the current timestamp.

After receiving $trans_{LN}$, SN checks whether the message has expired, then SN calculates $h_4 = \mathrm{Hash}(NodeID_{FD} \parallel t_b \parallel A_0)$. If $h_4 = h_3$, verified the message has not been tampered with. If the timeliness and authenticity of transaction information are verified by most of RNs, the authentication is determined to be passed by 2/3 SNs, denoted as $Pass_{FD}$; on the contrary, verified failed, denoted as $False_{FD}$.

Step 6. Identity registration information consensus and uplink stage of field device

After the authentication of FD has passed, LN packages ms into $Block_A$ and broadcasts it. After receiving $Block_A$, SN needs to link up ms and returns the authentication result to EG and FD.

Step 7. Update stage of behavior information and reputation value of consensus nodes

In the identity registration information uplink phase, the reputation value and behavior information table of the consensus node will be recorded and updated by LN, which based on the uplink behavior and results of the identity registration information of LN and SN, as shown in Table II.Evaluating the erroneous behavior of LN and SN is focused in this paper, therefore, when setting the weight value of the behavior attributes, a large weight assigned to the malicious behavior, the behavior weight assignment table is shown in Table III. Then LN updates the reputation rew_{LN} of new LN based on $rew_{LN} = (S \times \omega_1 - F \times \omega_2) \times (1 - r_{LN}) + r_{LN}$; LN updates the reputation rew_{RN} of SNs based on $rew_{RN} = (A_1 \times \omega_5 - G_f \times \omega_3 - G_{e_j} \times \omega_4) \times (1 - r_{RN}) + r_{RN}$, A_1 represents the number of times RN has reached normal consensus. Finally, the updated reputation value will be filled in Table II by LN.

TABLE III. ASSIGN WEIGHTS TO THE BEHAVIOR ATTRIBUTES OF THE LEAD AND SLAVE NODES

Behavior attribute	Weight
The behavior of LN identity registration information being linked	ω_1，（$\omega_1 \ll 0.5$）
The behavior of LN identity registration information not being linked	ω_2，（$\omega_2 \gg 0.5$）
The behavior of SN identity registration information consensus failed	ω_3，（$\omega_3 = \omega_4 > \omega_5$）
The behavior of SN repeatedly sending consensus messages	ω_4，（$\omega_4 = \omega_3 > \omega_5$）
The behavior of SN completing consensus	ω_5，（$\omega_5 < \omega_4 = \omega_3$）

C. Trust evaluation method based on comprehensive evaluation

The trust evaluation method in this article is based on the trust semi ring model. In the model, there is not only direct-interaction between the FD and EG, but also indirect-interaction between EG and R which R acts as intermediate nodes to assist.

1) Symbol description

This section provides an explanation of the meanings of the symbols used in trust evaluation, as shown in Table IV.

2) Calculate direct trust evaluate

EG uses SM4 based data integrity check digit generation mechanism for MW_{FD} and MW_{EG} to obtain MIC_{FD} and MIC_{EG}. EA verifies the consistency of MIC_{FD} and MIC_{EG}. EA uses Bayesian algorithm with logarithmic operation to calculate the direct trust value based on the consistency verification results[18-19].The calculation is shown in (1).

$$\mathrm{DT_{EG-FD}}(t) = \log_2\left(1 + \frac{\alpha_{\mathrm{EG-FD}}(t)+1}{\alpha_{\mathrm{EG-FD}}(t)+\beta_{\mathrm{EG-FD}}(t)+2}\right) \quad (1)$$

Where $\alpha_{EG-FD}(t)$ is the number of positive feedback which represents the number of times $MIC_{EG} = MIC_{FD}$ counted by the EA t from 0 to t; $\beta_{EG-FD}(t)$ is the number of negative feedback which represents the number of times $MIC_{EG} \neq MIC_{FD}$ counted by the EA from 0 to t.

TABLE IV. SYMBOLS USED IN THE TRUST EVALUATION METHOD

Name	Description
EG	Edge Gateway
EA	Edge Agent
FD	Field device
R	Route
MW_{FD}	Plain text of FD in direct trust evaluation
MW_{EG}	Plain text of EG in direct trust evaluation
MIC_{FD}	Check code of FD in direct trust evaluation
MIC_{EG}	Check code of EG in direct trust evaluation
DT_{EG-FD}	Direct trust value between FD and EG
RT_{EG-FD}	Recommendation trust value between FD and EG
T_{FD}	Comprehensive trust value of FD
$S_{RD-FD}(t)$	Recommended trust evaluation factor
ϕ_u	Uncertainty threshold
ϕ_c	Certainty threshold

3) Recommended trust evaluate

Step 1: Calculate the initial recommended trust value

According to the trust semi ring model, the recommended trust value between EG and FD in this paper is equal to ⊗ operation between EG and R, and between R and t FD : $RT_{EG-R-FD} = DT_{EG-R} \otimes DT_{R-FD} = DT_{EG-R} \cdot DT_{R-FD}$.

When there are multiple paths between EG and F, use the properties of ⊕ operation[20-22] to calculate the recommended trust value RT_{EG-FD} between EG and F, as shown in (2).

$$RT_{EG-FD} = RT_{EG-R_1-FD} \oplus ... \oplus RT_{EG-R_i-FD}$$
$$= \lambda_1\left(DT_{EG-R_1} \cdot DT_{R_1-FD}\right) + ... + \lambda_i\left(DT_{EG-R_i} \cdot DT_{R_i-FD}\right) \quad (2)$$

Where $\lambda_i = \frac{DT_{EG-R_i}}{\sum_{i=1}^{n} DT_{EG-R_i}}$, $(\lambda_1, ..., \lambda_i)$ represents the weight value of the recommended trust value on the path from EG to FD through the i-th routing node.

Step 2: Optimize and update initial recommended trust value

Recommended trust evaluation factor $S_{R-FD}(t) = 1 - \left(\sqrt{\frac{12(\alpha_{R-FD}(t')+1)}{(\alpha_{RD-FD}(t')+\beta_{R-FD}(t')+2)^2}}\right) \times \sqrt{\frac{(\beta_{R-FD}(t')+1)}{(\alpha_{R-FD}(t')+\beta_{R-FD}(t')+3)}})$ is introduced to measure the weight of each recommended value in this paper, the higher $S_{R-FD}(t)$, the more reliable recommendation trust evaluation is. Then update the recommended trust value base on (2). Then the recommended trust value will be sent to EA by EG. The calculation is shown in (3).

$$RT_{EG-FD}(t') = \sum_{k=1}^{n} \frac{DT_{R-FD}(t') \times S_{R-FD}(t')}{\sum_{k=1}^{n} DT_{R-FD}(t') \times S_{R-FD}(t')} \times RT_{EG-FD}(t) \quad (3)$$

n represents the total number of recommended device (router) participating in recommendation trust evaluation.

4) Comprehensive trust evaluate

Step 1: Calculate comprehensive trust value

Considering that most of the recommended trust values received by EA may be wrong when the proportion of malicious recommendation nodes(R)is high, which will lead to low accuracy of recommendation trust evaluation. The adaptive weights ω is introduced in this paper, the calculation of the comprehensive trust value T_{TE} of FD is shown in (4).

$$T_{FD} = \omega DT_{EG-FD}(t) + (1-\omega) RT_{EG-FD}(t) \quad (4)$$

Step 2: Determine trust level

After calculating the comprehensive trust value, EA divides the trust levels of TE. The uncertainty threshold of the trust level is ϕ_u , and the trust threshold is ϕ_c . The corresponding relationship between the trust level and the trust value range is shown in Table V.

TABLE V. RELATIONSHIP BETWEEN TRUST LEVEL AND TRUST VALUE RANGE

Trust level	Trust value range
Not-trusted	$[0,\phi_u)$
Uncertain	$[\phi_u,\phi_c)$
Trusted	$[\phi_c,1]$

III. TESTING

A. System construction

According to the framework, the field device authentication test and verification system is built in the industrial edge computing environment. Table VI describes the hardware used in this system. The verification test system is shown in Fig.2.

TABLE VI. AUTHENTICATION TESTS VERIFY THE HARDWARE EQUIPMENT USED BY THE SYSTEM

Hardware	Num.	Equipment Model
FD	3	CC2530
EG	1	S3C2400
R	2	CC2530
ES	5	Raspberry Pie 4 Model B 4G
Console	1	Intel(R)Core(TM)i5 CPU@1.60GHz
S	1	H3C IE4320-10S

B. Performance testing of field device authentication method

1) Testing the time cost of authentication

In this paper, 4, 5, and 6 consensus nodes are used as examples to calculate the authentication time for FD to undergo 25 rounds of authentication. After testing, the authentication time T_{Ide} for 4 consensus nodes is 594.1ms, when there are 5 consensus nodes T_{Ide} is 600.2ms, when there are 6 consensus nodes T_{Ide} is 603.9ms, average T_{Ide} is 599.4ms.

2) Testing the time cost of consensus confirmation

Based on the test results of authentication time, 5 consensus nodes were used as test condition. The consensus time T_{Con} for 6 rounds of authentication for 1, 2, and 3 FDs have been calculated respectively. After testing, the T_{Con} of

1 FD is 541.5ms, the T_{Con} of 2 FDs is 539.7 ms, the T_{Con} of 3FDs is 545.6ms, average T_{Con} is 544.2ms.

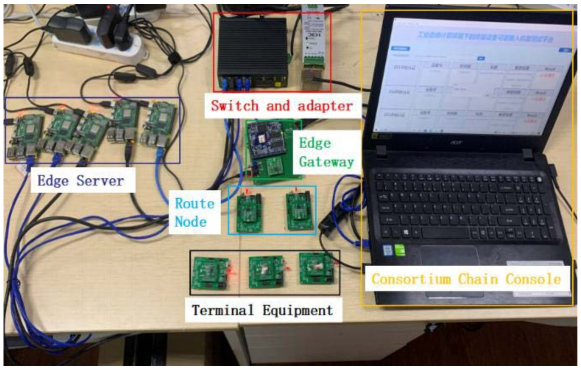

Fig. 2. Field device authentication verification test system

3) Comparative testing of consensus confirmation time

An industrial edge computing network with five consensus nodes was built, and the consensus confirmation time has been compared with PBFT and RBFT,as shown in Figure 3.

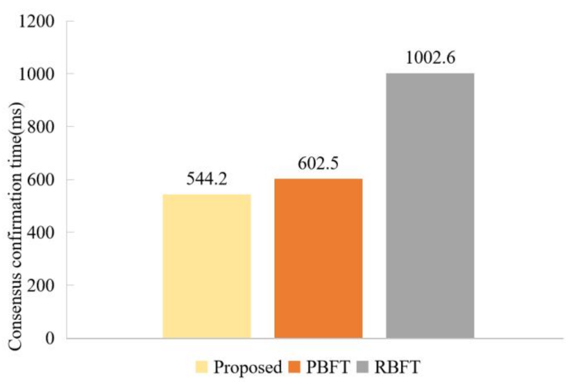

Fig. 3. Comparison of consensus confirmation time

C. Testing of trust evaluation method

1) Testing recommended trust evaluation factor $S_{\mathrm{R-FD}}^{t}$

$S_{\mathrm{R-FD}}^{t}$ is introduced to measure the weight of each recommendation value in this paper, $S_{\mathrm{R-FD}}^{t}$ minimized the deviation caused by uncertain recommendation values in the calculation of comprehensive trust values. The trust values with and without the introduction of $S_{\mathrm{R-FD}}^{t}$ were calculated separately, the test results shown in Figure 4.

2) Testing trust evaluation effectiveness

The assessment of field device trust level is based on the range within which the trust value falls. Therefore, for improving the accuracy of trust level assessment, the selection of trust threshold ϕ_c and uncertainty threshold ϕ_u have been tested for the improvement of the accuracy of trust level assessment. The relationship between FD trust values and trust thresholds: When $\phi_u = 0.709,\ \phi_c = 0.909$ and $\phi_u = 0.689,\ \phi_c = 0.889$, there is exist the behavior of not dividing the effective trust value into corresponding trust levels that is not suitable as a trust threshold for trust evaluation systems; when $\phi_u = 0.641,\ \phi_c = 0.841$, there is a risk of dividing invalid trust values into uncertain trust levels, which is not suitable as a trust threshold for trust evaluation systems.

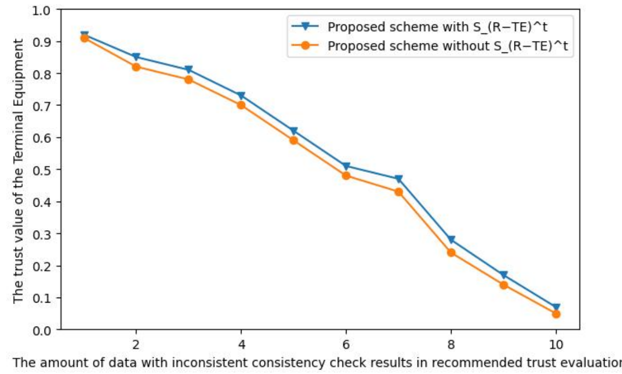

Fig. 4. The effect of recommendation trust evaluation factor

IV. Analysis and Discussion

A. Analysis of field device authentication method

1) Analyzing the time cost of authentication

With the increase of the number of consensus nodes, the time consumed by the authentication method of FD will increase slightly, so there is no need to deploy too many consensus nodes. At the same time, the authentication only involved addition, multiplication encryption and hash computation with shorter word length output, which ensures that the time cost of identity authentication is maintained at 600ms, which can be better applied to industrial edge computing networks.

2) Analyzing the time cost of consensus confirmation

The increase of FD will not lead to a significant increase in consensus time, as the introduction of a consensus node selection mechanism will set a threshold for consensus time, ensuring that nodes who participating in the consensus algorithm in each round complete the consensus within a certain consensus time.

3) Comparative analyzing of consensus confirmation time

Distinguished from the traditional PBFT and RBFT where all nodes participate in the consensus, in this paper high-scoring nodes are selected to participate in the consensus based on their reputation values, dynamically updating the reputation values, which increases the success rate of consensus and shortens the time for consensus confirmation. Therefore, this scheme is suitable for time sensitive industrial edge computing networks.

B. Analysis of trust evaluation method

1) Analyzing recommended trust evaluation factor $S_{\mathrm{R-FD}}^{t}$

Since $S_{\mathrm{R-FD}}^{t}$ is related to the number of positive and negative feedback, $S_{\mathrm{R-FD}}^{t}$ is positively correlated with the number of positive feedback. The larger $S_{\mathrm{R-FD}}^{t}$, the more reliable the recommendation trust evaluation is. In Figure 4 shown that the introduction of $S_{\mathrm{R-FD}}^{t}$ can effectively reduce the weight of malicious recommendation trust value, and thus reduce the error between the calculated trust value and the true trust value.

2) Analyzing trust evaluation effectiveness

From the test results of threshold selection, it can be seen that when $\phi_u = 0.666$, $\phi_c = 0.866$, the trust evaluation system can divide the trust levels of all valid trust values into distrusted data rates of 0.10, 0.20, 0.30, and 0.40, besides there is no behavior of dividing the trust levels into invalid trust values, this system can effectively identify malicious terminal device in industrial edge computing environment.

V. CONCLUSIONS

This paper proposed a trusted access mechanism for field device in industrial edge computing environment, the mechanism includes authenticating the identity of field device based on the reputation value and assessing the trust of field device based on the trust value, which provided a distributed, traceable, real-time trusted access to industrial networks. The authentication test and verification system and trust evaluation system of field device in the industrial edge computing environment has been built. The test results showed that this system can verify the legitimacy of field device identity and detect security attack behavior in short time besides with low storage cost. It can also calculate the trust value and evaluate the trust level of field device, and detected security attack behavior. It improved the security protection capability of industrial edge computing.

ACKNOWLEDGMENT

The paper is the National Key Research and Development Program of China (2021YFB3301000) and the Chongqing Natural Science Foundation Innovation and Development Joint Fund project （CSTB2023NSCQ-LZX0123）.

REFERENCES

[1] C. N. Shen, “Research progress of edge computing security and privacy protection,” Network Security and Data Governance, vol. 41, no. 08, pp. 41-43, Aug 2022.

[2] J. L. Zhang, Y. C. Zhao, and B. Chen, “A survey of data security and privacy protection in edge computing,” Journal of Communications, vol. 39, no. 3, pp. 2-5, 2018.

[3] F. Zhang, X. Jiang. “The zero-trust security platform for data trusteeship,” in 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), Changsha, China, pp. 1014-1017, Aug. 2021.

[4] L. Chen, Z. Dai, M Chen, N. G. Li, “Research on the security protection framework of power mobile internet services based on zero trust,” 6th International Conference on Smart Grid and Electrical Automation (ICSGEA), Kunming, China, pp. 65-68, July 2021.

[5] V. Krishnan, S. Sreeja, “Zero trust-based adaptive authentication using composite attribute set,” IEEE 3rd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), Bangalore, pp. 5-15, Dec. 2021.

[6] M. Sarvabhatla, C. S. Vorugunti, “A secure biometric-based user authentication scheme for heterogeneous WSN,” 2014 Fourth International Conference of Emerging Applications of Information Technology, Kolkata, India, pp. 367-372, Mar. 2015.

[7] J. L. Tsai, N. W. Lo, “A privacy-aware authentication scheme for distributed mobile cloud computing services,” IEEE Systems Journal, vol. 9, no. 3, pp. 805-815, July 2015.

[8] A. Ben, M. Abid, A. Meddeb, “A privacy-preserving authentication scheme in an edge-fog environment,” 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, pp. 1225-1231, Dec. 2018.

[9] K. Kaupr, S. Garg, G. Kaddoum, M. Guizani, D. N. K. Jayakody, “A lightweight and privacy-preserving authentication protocol for mobile edge computing,” IEEE Global Communications Conference (GLOBECOM), Hawaii, USA, pp. 52-63, Feb. 2019.

[10] L. Zhang, X. Y. Wei, X. P. Liu, “A trust evaluation algorithm for IoT edge servers based on collaborative reputation and device feedback,” Journal of Communications. China, vol. 43, no. 02, pp. 118-130, Jan. 2022.

[11] W. Kong, X. Li, L. Hou, J. Yuan, Y. Gao, Y. Shui, “A reliable and efficient task offloading strategy based on multifeedback trust mechanism for IoT edge computing,” IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13927-13941, Aug. 2022.

[12] M. B. Monir, T. Abdelkader, E. Horbaty, “Trust evaluation of service level agreement for service providers in mobile edge computing,” 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, pp.362-369, Mar. 2019.

[13] S. Li, I. Doh, K. chae, “Non-redundant indirect trust search algorithm based on a cross-domain trust model in content delivery network,” 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), pp. 72-77, Mar. 2017.

[14] Z. Ma, X. Wang, K. Deepak, K. Haneef, Z. Wang, “A blockchain-based trusted data management scheme in edge computing,” IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2013-2021, Mar. 2020.

[15] Z. Ma, J. Meng, J. Wang, Z. Shan, “Blockchain-based decentralized authentication modeling scheme in edge and IoT environment,” IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2016-2023, Feb. 2021.

[16] G. Sun, M. Dai, J. Sun, H. Yu, “Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain,” IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6257-6272, April 2021.

[17] V. Nguyen, “Scalable distributed random number generation based on homomorphic encryption,” IEEE International Conference on Blockchain, Atlanta, GA, USA, pp. 572-579, July 2019.

[18] G. Bai, H. Fu, W. Li, X. Wu, “Differential power attack on SM4 block cipher,” 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, pp.1494-1497, Aug. 2018.

[19] A. Xu, G. Liu, Y. M. Xun, C. Wang, J. Chang, “Research and application of industrial control protocol security based on national security system,” Automation Panorama, vol. 38, no. 01, pp. 99-103, Jan. 2021.

[20] D. Rough, D. P. St, A. Wilson, “Commonshare: A new approach to social reputation for online collaborative communities,” Social Science Computer Review, vol. 8, no. 15, pp. 852-864, July 2021.

[21] G. D. Tormo, F. G. Marmol, M. Perezg, “Dynamic and flexible selection of a reputation mechanism for heterogeneous environments,” Future Gener Comput System, vol. 49, pp. 113-124, Aug. 2015.

[22] Y. Han, Z. Q. Shen, C. Y. Miao, S. X. Liang, C. Leung,D.Niyato, “A survey of trust and reputation management systems in wireless communications,” Proc IEEE, vol. 98, no. 10, pp.1755-1772, Oct. 2010.

[23] X. Pan, L. Y. Yuan, M. M. Huang, “Cross domain trust evaluation model for the Internet of Things based on blockchain and domain trust,” Computer Engineering, vol.49, no. 05, pp. 181-190, Jan. 2023.