Hindawi
International Journal of Intelligent Systems
Volume 2023, Article ID 8899697, 11 pages
https://doi.org/10.1155/2023/8899697

Research Article

A Hierarchical Authentication System for Access Equipment in Internet of Things

Hui-Juan Zhang,[1,2] **Shen He**,[1,2] **Jia Chen**,[1,2] **Kai Yang**,[1,2] **Peng Ran**,[1,2] **and Jiake Chen**[1,2]

[1]*Research Institute of China Mobile Communications Corporation, Beijing 100032, China*
[2]*Research Institute of Safety Technology, Beijing 100032, China*

Correspondence should be addressed to Hui-Juan Zhang; zhanghjyusheng@163.com

Received 21 January 2023; Revised 30 April 2023; Accepted 11 May 2023; Published 24 May 2023

Academic Editor: Lianyong Qi

With the development of Internet of Things (IoT) technology, massive heterogeneous equipment involving all walks of life has been connected to networks. However, many current authentication methods have poor robustness and cannot ensure the safety of access equipment due to the complexity and uncertainty of the network environment. To deal with this problem, a hierarchical authentication system was proposed in this paper. First, an equipment identification method (EIM), using stack denoising autoencoders (SDAs), is developed to weaken the uncertainty to recognize the type of access equipment. Second, an equipment authentication method (EAM), based on the identification result and similarity theory, is designed to improve the verification accuracy to guarantee the credibility of access equipment. Third, the proposed hierarchical authentication system was tested in a real access platform. The experimental results demonstrated the satisfactory performance of this proposed hierarchical authentication system.

1. Introduction

With the development of computer technology and sensor technology, the Internet of Things (IoT) has become a bridge between virtual and reality worlds, which plays a vital role in human production and life [1–3]. However, the network environment is increasingly complex and contains various uncertainties due to the access of massive heterogeneous equipment [4–6]. The attacker can utilize the illegal equipment to steal important data information and even control the equipment to make the collapse of the entire IoT platform, which will cause the irretrievable damage [7–10]. For example, attackers can attack smart devices in our family to steal important information and even attack devices with cameras to monitor us. Thus, how to authenticate the identity of access equipment to ensure the safety of the IoT is an urgent problem.

To verify the equipment identity, Fragkos et al. adopted the uniqueness and unpredictability of physically unclonable functions (PUFs) to perform the device authentication to ensure the identity legality [11]. Tremlet and Jones utilized PUFs to produce the keys and access passwords of devices for authentication [12]. Yang et al. proposed an authentication mechanism based on a trusted token to verify device identity using the load-carrying key [13]. However, these techniques in [11–13] depend on the hardware, which limits their applications in IoT environment. Considering the ease of deployment, Das et al. designed a lightweight authentication method, using the elliptic curve cryptography (ECC) and a collision-resistant one-way cryptographic hash function, to realize the identity authentication [14]. Moreover, Badhib et al. proposed a lightweight bidirectional authentication method to detect equipment identity [15]. In this authentication method, the hash function was regarded as the core encryption module, which has high security. In addition, a key authentication protocol based on dynamic update of group was developed, which adopted the asynchronous secret sharing mechanism and Diffie–Hellman key exchange mechanism to identify the validity of the equipment [16]. Meanwhile, some approaches based on the credibility of equipment have been investigated. For example, public key infrastructure (PKI) is a typical trust model in [17–21]. PKI relies on the trusted third-party organizations or certificates to organize the trust relationship to verify the device identity [22–24]. In addition, other model based on the credibility can be found in [25, 26]. However, in these above methods [14–26], the predistribution of a key, protocol, or trust certificate must be completed before network deployment or equipment access and cannot dynamically change with the change of network size. Therefore, these methods have poor adaptability and scalability.

For improving adaptability and scalability, authentication mechanisms based on the dynamic behaviors of equipment have proposed [27]. For example, Singh et al. adopted the multivariate correlation analysis technology to analyze the data packets in network layer [28]. Then, the legitimacy of the equipment can be confirmed by analyzing the correlation between network traffic features. Wang et al. established a device fingerprint database by collecting the dynamic and static information of equipment [29]. Then, the device to be validated can match with the fingerprint database to realize the identity authentication. Meanwhile, Kamvar and Schlosser adopted the EigenTrust model to calculate the interaction trust value of nodes to evaluate the credibility of equipment [30]. Although the above method based on the dynamic behavior information can identify abnormal devices, they cannot effectively authenticate unknown devices. Recently, the development of artificial intelligence algorithm provides a new solution for some problems [31–33]. Chen et al. proposed an authentication mechanism based on the credibility of cross-layer behaviors of access devices. The *k*-means algorithm was used to classify to determine the trust level of these devices, using the behavior parameters of access devices in different network layers. Experimental results revealed that this mechanism has better authentication performance comparing with the traditional methods. Moreover, Lin et al. used a Bayesian network to quantize the credibility of access equipment [34]. For the Bayesian network, the direct trust value, recommendation trust value, and historical statistics trust value of these devices were taken as the input, and a syncretic trust value was regarded as the output. When the trust value is higher than the preset threshold, the access request was granted, and vice versa. The results indicated that the proposed method can prevent the interaction with untrusted device to improve the security and reliability of the IoT. These above methods [34, 35] have achieved the success on verifying the identity of equipment. However, the IoT environment consists of the unpredictable uncertainties due to the increasing functionality and complicated interaction behaviors of devices. These above methods have poor accuracy and fail to meet the current certification requirements for IoT.

Motivated by the above discussion, to improve the certification accuracy in uncertainty IoT environment, a hierarchical authentication system was proposed in this paper. First, an equipment identification method (EIM), using the stack denoising autoencoders (SDAs), is developed to weaken the uncertainty to recognize the equipment type. Second, based on the identification result and similarity theory, an equipment authentication method (EAM) is designed to further improve the verification accuracy to achieve the credibility of access equipment in the IoT. Third, the proposed hierarchical authentication system was tested in real applications based on a certain access platform of China Mobile. The experimental results demonstrated the satisfactory performance of the proposed hierarchical authentication system.

The outline of this paper is organized as follows. The proposed hierarchical authentication system is given in Section 2. In Section 3, the experimental results of the hierarchical authentication system were discussed, and the practical application in certain access platform is provided in Section 4. The conclusions are given Sections 5. Finally, an Table 1, including the main symbols appearing in this paper, was given to increase the readability.

2. Hierarchical Authentication System for Access Equipment

In this section, a hierarchical authentication system was developed for the identity verification of access equipment in the IoT. As shown in Figure 1, the variables of equipment in multiple industries (smart city, smart home, and so on) are collected, which consists of dynamic behavior and static information of equipment. An EIM is proposed to identify the equipment type using the collected variables. Then, based on the identification result, an EAM can verify the equipment identity. Finally, the certification results are displayed on the screen to provide warning information for the workers. The workers can take corresponding actions to deal with the warning. Next, the collected variables of equipment are given. Meanwhile, EIM and EAM are introduced in detail.

2.1. Variable Collection of Access Equipment. To improve the reliability of authentication results, the dynamic behavior and static information of access equipment are collected, consisting of the data of the network layer and the application layer. The flow data in the network layer can be captured by using the Wireshark, which will be packaged as the pcapng file. Then, the pcapng file can be resolved and stored into the database, where the collected characteristic variables include the destination IP, destination port, source IP, source port, and so on. Moreover, the data variables of the application layer can be acquired by gathering the history log of equipment in the database.

Such as application industry, node types, operating system, service invocation type, and so on. The number of obtained data variables is 23 and can be summarized in Table 2.

2.2. Equipment Identification Method (EIM). At present, many methods have poor robustness and fail to satisfy the authentication requirements due to the complexity and uncertainty of the IoT environment and the interaction

Table 1: The summary of main symbols in this manuscript.

Number	Symbol	From	Description
1	$\bar{\mathbf{x}}$	Formula (1)	The partially destroyed version of raw training set
2	$\mathbf{x}$	Formula (1)	The raw training set
3	x_i	Formula (1)	The *i*th input variable
4	$\bar{x}_i$	Formula (1)	The destroyed variable of *i*th input variable
5	r_i	Formula (2)	The random number
6	p	Formula (2)	Corruption factor
7	$\mathbf{w}_1$	Formula (3)	The weight matrix of encoder
8	$\mathbf{b}_1$	Formula (3)	The bias vector of encoder
9	$\mathbf{\Phi}$	Formula (4)	The input vector $\mathbf{\Phi}$ of decoder
10	$\bar{\mathbf{w}}_1$	Formula (4)	The weight matrix of decoder
11	$\bar{\mathbf{b}}_1$	Formula (4)	The bias vector of decoder
12	$\mathbf{z}$	Formula (5)	The output of decoder
13	η	Formula (7)	The learning rate
14	$\mathbf{W}_1$	Formula (7)	The set of weight matrices
15	$\mathbf{B}_1$	Formula (7)	The set of bias vectors
18	$\mathbf{u}$	Formula (8)	The actual output of EIM
19	$\mathbf{u}'$	Formula (8)	The target output of EIM
20	Δ_l	Formula (10)	The gradient of $\partial L/\partial \boldsymbol{\psi}_l$
21	$\boldsymbol{\psi}_l$	Formula (10)	The input vector of *l*th hidden layer
22	$\mathbf{w}_l$	Formula (11)	The weight matrix of *l*th hidden layer
23	$\mathbf{b}_l$	Formula (11)	The bias vector of the *l*th hidden layer
24	u_j	Formula (12)	The *j*th device type
25	w_{ij}	Formula (12)	The connection weight of *i*th hidden neuron and *j*th hidden neuron
27	$u\ (t)$	Formula (13)	The identification result at time *t*
28	$\boldsymbol{\gamma}$	Formula (14)	The average value of each variable
29	ζ	Formula (15)	The preset value
30	q	Formula (16)	The number of batchsize
31	v_i	Formula (16)	The number of input nodes of the *i*th DA
32	s_i	Formula(16)	The number of hidden nodes of the *i*th DA
33	Q_R	Formula (19)	The number of correct classification of sample
34	Q	Formula (19)	The number of total samples
35	Q_F	Formula (19)	The number of false positives sample
36	Q_N	Formula (19)	The number of negative sample

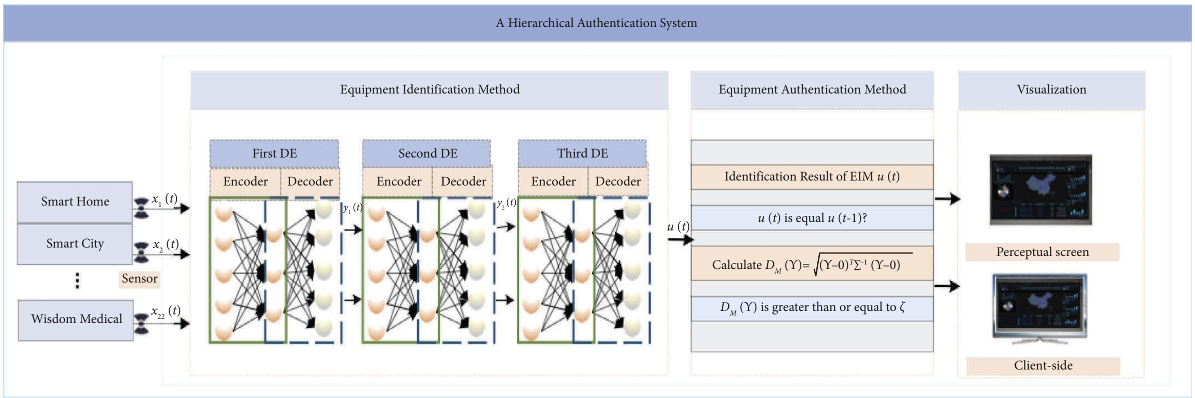

A Hierarchical Authentication System
Equipment Identification Method
Equipment Authentication Method
Visualization
Smart Home
Smart City
Wisdom Medical
Sensor
x_1 (t)
x_2 (t)
x_{22} (t)
First DE
Second DE
Third DE
Encoder
Decoder
Encoder
Decoder
Encoder
Decoder
y_1 (t)
y_2 (t)
u (t)
Identification Result of EIM u (t)
u (t) is equal u (t-1)?
Calculate $D_M(\Upsilon)=\sqrt{(\Upsilon-0)^T\Sigma^{-1}(\Upsilon-0)}$
$D_M(\Upsilon)$ is greater than or equal to ζ
Perceptual screen
Client-side

Figure 1: The framework of the proposed hierarchical authentication system.

between devices. As a kind of deep learning, SDAs can reconstruct the clean data from the partially destroyed version, which can weaken the effectiveness of uncertainty [36]. Therefore, in the proposed EIM, SDAs are used to recognize the access device type.

SDAs are stacked by several base-building units DA layer by layer. As shown in Figure 1, DA contains an encoder and a decoder, and the input vector of the encoder is

$$\bar{\mathbf{x}} = \mu\mathbf{x}, \tag{1}$$

Table 2: The collected variables of the proposed hierarchical authentication system.

Num	Collected variable	Input/output variable	From	Description
1	Destination IP	Input variable	Network layer	Destination IP of access equipment
2	Destination port	Input variable	Network layer	Destination IP port
3	Message type	Input variable	Network layer	Message type: TCP and UDP
4	Source IP	Input variable	Network layer	Source IP of access equipment
5	Source port	Input variable	Network layer	Source IP port
6	Packet length	Input variable	Network layer	Average packet length
7	Sequence number	Input variable	Network layer	Ensuring the order of transmission
8	ACK	Input variable	Network layer	Acknowledgement pointer flag
9	URG	Input variable	Network layer	Urgency pointer flag
10	Number of packets	Input variable	Network layer	Received the number of packets per second
11	Application industry	Input variable	Application layer	Equipment application industry
12	Number of service invocation	Input variable	Application layer	Number of service invocation of equipment
13	Warning number	Input variable	Application layer	Number of warning number of equipment
14	Node types	Input variable	Application layer	Directly connected devices, gateway devices, and so on
15	Protocol type	Input variable	Application layer	MQTT, LwM2M, HTTP, and so on
16	Bearer network type	Input variable	Application layer	WIFI, 3G, 4G, 5G, NB, and so on
17	Service invocation type	Input variable	Application layer	Service invocation type of equipment
18	Operating system	Input variable	Application layer	Linux, windows, android, and so on
19	Network operator	Input variable	Application layer	Mobile, telecom, unicom, and so on
20	Internet access	Input variable	Application layer	WiFi, cellular, and NB-loT
21	Daily flow	Input variable	Application layer	Total daily traffic of the device
22	Activation	Input variable	Application layer	Daily standby duration of the device
23	Equipment type	Output variable	Application layer	Equipment type

where $\bar{\mathbf{x}} = [\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{22}]$ is the partially destroyed version of raw training set $\mathbf{x} = [x_1, x_2, \ldots, x_{22}]$ of access device, x_i represents the ith input variable and $\bar{x}_i$ represents the corresponding destroyed variable, u can be given as

$$\mu = \begin{cases} 0, r_i < p \\ 1, r_i \geq p \end{cases}, r_i \in (0, 1), \tag{2}$$

where r_i represents the random number and p is the corruption factor. The output of encoder is

$$\mathbf{y}_1 = \frac{1}{\left(1 + e^{-\left(\mathbf{w}_1 \bar{\mathbf{x}} + \mathbf{b}_1\right)}\right)}, \tag{3}$$

where $\mathbf{w}_1$ is the weight matrix of encoder, $\mathbf{b}_1$ is the bias vector of the encoder. The input vector $\mathbf{\Phi}$ of the decoder is

$$\mathbf{\Phi} = \bar{\mathbf{w}}_1 \mathbf{y}_1 + \bar{\mathbf{b}}_1, \tag{4}$$

where $\bar{\mathbf{w}}_1$ is the weight matrix of decoder, $\bar{\mathbf{b}}_1$ is the bias vector of decoder. The output $\mathbf{z}$ of the decoder is

$$\mathbf{z} = \frac{1}{\left(1 + e^{-\mathbf{\Phi}}\right)}. \tag{5}$$

The loss function of DA can be given as

$$l_{DA} = \frac{1}{2} \|\mathbf{x} - \mathbf{z}\|^2, \tag{6}$$

where the error is the difference between the output of the decoder and the original input data. Therefore, DA can recover the clean sample from the corrupt sample, which reveals that DA has a robustness performance for the noise and uncertainty. The relevant parameters ($\mathbf{w}_1$, $\mathbf{b}_1$, $\bar{\mathbf{w}}_1$, $\bar{\mathbf{b}}_1$) of DA can be updated by unsupervised algorithm

$$\begin{cases} \mathbf{W}_1 = \mathbf{W}_1 - \eta \dfrac{\partial \mathbf{z}}{\partial \mathbf{W}_1} (\mathbf{x} - \mathbf{z}), \\ \\ \mathbf{B}_1 = \mathbf{b}_1 - \eta \dfrac{\partial l}{\partial \mathbf{\Phi}_1} \dfrac{\partial \mathbf{\Phi}_1}{\partial \mathbf{B}_1}, \end{cases} \tag{7}$$

where $\mathbf{W}_1 = (\mathbf{w}_1, \bar{\mathbf{w}}_1)$ and $\mathbf{B}_1 = (\mathbf{b}_1, \bar{\mathbf{b}}_1)$, $\eta \in (0, 1)$ is the learning rate. When the first DA is trained, the output layer of the decoder can be discarded. Then, the output vector of the encoder is regarded as the raw input of the next DA. In this way, multiple DAs are stacked layer by layer to build SDAs. Finally, the label layer of equipment type is added, which can be used to fine-tune the entire EIM. The loss function L of SDAs can be defined as

$$L_{\text{SDA}} = \frac{1}{2} \|\mathbf{u} - \mathbf{u}'\|^2, \tag{8}$$

where $\mathbf{u}$ represents the actual output of EIM, $\mathbf{u}'$ is the target output of EIM. Then, the relevant weights and biases in EIM can be updated

$$\begin{cases} \mathbf{W}_i = \mathbf{W}_l + \eta \Delta \mathbf{W}_l \\ \mathbf{b}_l = \mathbf{b}_l + \eta \Delta \mathbf{b}_l \end{cases}, \tag{9}$$

where

$$\begin{cases} \Delta \mathbf{W}_l = -\boldsymbol{\delta}_l \mathbf{y}_l, \\ \Delta \mathbf{b}_l = -\boldsymbol{\delta}_l. \end{cases} \tag{10}$$

$\Delta_l = \partial L/\partial \boldsymbol{\psi}_l$, $l = 1, 2, \ldots, m, m+1$, the $(m+1)$ th layer is the output layer of EIM, $\boldsymbol{\psi}_l$ is the input vector of each hidden layer.

The testing set is regarded as the input of EIM, the output $\mathbf{y}_0$ of input layer is

$$\begin{gathered} \mathbf{y}_l = \frac{1}{\left(1 + e^{-\boldsymbol{\psi}_l}\right)}, \\ \boldsymbol{\psi}_l = \mathbf{w}_l \mathbf{y}_{l-1} + \mathbf{b}_l, \end{gathered} \tag{11}$$

where $\mathbf{w}_l$ is the weight matrix of lth hidden layer and $(l+1)$ th hidden layer, $\mathbf{b}_l$ are the bias vector of the lth hidden layer, $\mathbf{y}_0 = \bar{\mathbf{x}}$. the recognition output of EIM is

$$u_j(t) = \frac{e^{w_{ij} y_i}}{\sum_{j=1}^{n} e^{w_{ij} y_i}}, \tag{12}$$

where u_j represents the jth device type, w_{ij}, is the connection weight of ith hidden neuron and jth hidden neuron, n is the number of device types.

Remark 1. Based on the collected variables, the proposed EIM is used to determine the device type, which can effectively alleviate the impact of uncertainty with the powerful robustness. Therefore, comparing with some authentication methods, this EIM has the better identification accuracy.

2.3. Equipment Authentication Method (EAM).

To verify the validity of access devices, an EAM, based on the identification result of EIM and similarity theory, is proposed. In this proposed EAM, the access device implements the evaluation for the first time:

$$u(t) = u(t-1), \tag{13}$$

where $u\ (t)$ represents the identification result at time t and $u\ (t-1)$ is the identification result at time $(t-1)$. When the identification result at time t is equal to the identification result at time $(t-1)$, the device is trustworthy. Otherwise, based on the similarity theory, the validity of the device can be re-judged. The similarity can be computed as

$$D_M(\Upsilon) = \sqrt{(\Upsilon - \mathbf{o})^T \sum^{-1} (\Upsilon - \mathbf{o})}, \tag{14}$$

where q variables selected from the input variables constitute the vector $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_q)$, $\mathbf{o} = (o_1, o_2, \ldots, o_q)$ is the average value of each variable, $\sum(.)$ is the covariance calculation.

$$D_M(\Upsilon) \geq \zeta. \tag{15}$$

When device certification succeeds, ζ is a preset value. By calculating the similarity, the authentication failure caused by classification error can be effectively distinguished, so that EAM can further improve the authentication accuracy.

Remark 2. The proposed EAM can avoid the error of EIM, by again evaluating the credibility of access devices, to further improve the robustness for the uncertainty.

Remark 3. Based on the EIM and EAM, the proposed hierarchical authentication system can effectively alleviate the impact of uncertainty and has the satisfying certification accuracy. Moreover, the equipment standard $u\ (t)$ that EIM fails to authenticate and EAM successfully authenticate can be corrected by the relabeled personnel to facilitate the next certification.

2.4. The Implementation of Hierarchical Authentication System.

To analyze the practicability of the proposed hierarchical authentication system, the computational cost will be discussed. The computation involves two parts: the computational complexity of EIM and EAM. For EIM, the computational complexity of base-building unit DA can be given as

$$T_i = T_i^1 + T_i^2, \begin{cases} T_i^1 = O\left(v_i^* s_i + s_i + v_i s_i\right) = O\left(s_i\right) \\ T_i^2 = O\left(q^* c^* l\right) \end{cases}, \tag{16}$$

where v_i is the number of input nodes of the ith DA and s_i is the number of hidden nodes of the ith DA. q is the number of batch sizes, c is the time complexity of a sample gradient, l is the iteration, T_i^1 is the calculation amount of the forward propagation process of DA, and T_i^2 is the calculation amount of the backpropagation propagation process of DA. The computational complexity T_{EIM} of EIM is

$$T_{\text{EIM}} = \sum_{i=1}^{m} T_i. \tag{17}$$

The computational complexity T_{EAM} of EAM is

$$T_{\text{EAM}} = O\left(c_q^2\right). \tag{18}$$

Therefore, the computational complexity of the proposed hierarchical authentication system is the sum of T_{EIM} and T_{EAM}. For our device authentication scenario, the number of input features obtained is 22, and the number of hidden layers and the hidden nodes is comparatively simple than image recognition. Therefore, the proposed hierarchical authentication system algorithm does not require the huge computing resources and power consumption, which can be well arranged in practice.

3. Results and Discussion

To demonstrate the effectiveness of hierarchical authentication system, the simulation examples are discussed in this section. The simulations are run on Windows 10.0 operating system with a clock speed 2.6 GHz, 4 GB RAM, and Python 3.6. Moreover, to evaluate the performance of this hierarchical authentication system, the accuracy, false positive rate, and false negative rate are introduced

$$\begin{cases} P_{\mathrm{IA}} = \left(\dfrac{Q_R}{Q}\right) \times 100\%, \\ P_{\mathrm{FP}} = \left(\dfrac{Q_F}{Q_p}\right) \times 100\%, \\ P_{\mathrm{FN}} = \left(\dfrac{Q_M}{Q_N}\right) \times 100\%, \end{cases} \tag{19}$$

where P_{IA} is the accuracy, P_{FP} is the false positive rate, P_{FN} is the false negative rate, Q_R is the number of correct classifications of samples, Q is the number of total samples, Q_F is the number of false positive samples, Q_P is the number of positive samples, Q_M is the number of false negative samples, and Q_N is the number of negative samples.

3.1. Equipment Type Identification of EIM. The collected 22 variables are regarded as the input of EIM, and the equipment type is considered as the output. In order to demonstrate the performance of EIM, two experiments are performed: A-64 kinds of equipment and B-128 kinds of equipment.

In example A, the number of training samples is 10000 and the number of testing samples is 3000. The hidden layer of EIM is 4 and the number of nodes at every layer is 256, 236, 128, and 64. The corruption factor p is 0.02 and the learning rate in EIM is 0.05. In example A, the number of training samples is 10000 and the number of testing samples is 3000. The hidden layer of EIM is 4 and the number of nodes at every layer is 256, 236, 128, and 64. The corruption factor p is 0.02 and the learning rate in EIM is 0.05.

The testing results of EIM for the 64 kinds of equipment in Example A are shown in Figure 2. In Figure 2, it displays the classification results between EIM and the target. It can be seen that this EIM can achieve the good equipment classification. To further reveal the performance of the proposed EIM, the results are compared with the stacked autoencoder (SAE), deep belief network (DBN), support vector machine (SVM), k-means, and BP network. To make the comparisons meaningful, all results are the average values of 50 trials. The comparison results of different methods are displayed in Figure 3, and the details of the comparison are shown in Table 3.

As shown in Figure 3, it represents the identification accuracy, FP rate, and FN rate of several methods in Example A. According to Figure 3 and Table 3, the performance of deep learning algorithm (EIM, SAE, and DBN) is the better than nondeep learning algorithms (SVM, k-means, and BP network). Especially, the accuracy of the proposed EIM is 0.88 and higher than other deep learning and the nondeep learning algorithms. Meanwhile, EIM owns the lowest FP rate (0.11) and FN rate (0.09) than that of all methods. Based on the above analysis, the proposed EIM can be used to weaken the uncertainty with a better robustness than the other algorithms.

In example B, the number of training samples is the same as the example A, where the training samples are 20000 and the testing samples are 6000. Moreover, the hidden layer of EIM is 5, and the number of nodes is set to 320, 200, 180, 120, and 50. The corruption factor p is 0.01 and the learning rate in EIM is 0.1.

The testing results are displayed in Figure 4. The results of Figure 4 reveal that the proposed EIM can obtain good identification for the equipment type. Furthermore, to testify the advantages of EIM, the results are compared with some other algorithms: SAE, DBN, SVM, k-means, and BP network. The accuracy, FP rate, and FN rate are also displayed in Figure 5, and the comparison among EIM and other methods is summarized in Table 4.

Based on the results in Figure 5 and Table 4, it can be seen that the accuracy of the proposed EIM is the 0.84 and more than that of the other algorithms. Moreover, the FP rate is the 0.12 and the FN rate is the 0.10, which are less than those of the other algorithms. Therefore, the proposed EIM can achieve a satisfactory recognition performance.

3.2. Equipment Identity Authentication of EAM. Based on the recognition results, the proposed EAM can verify the device identity. The similarity index variables are packet length, the number of packets, the number of service invocations, service invocation type, daily flow, and activation. The preset value ζ is 0.075. To adequately assess the performance of EAM, this EAM is used for the identity authentication of the 64 kinds of equipment (Example C) and the 128 kinds of equipment (Example D), respectively. The certification results are compared with the SAE, DBN, SVM, k-means, and BP network.

The comparisons are given in Figure 6. In Figure 6, the accuracy of the proposed EAM is higher than the EIM. Meanwhile, the FP rate and FN rate of the EAM are lower comparing with the EIM. Therefore, it can reveal that the EAM further improves the certification performance of EIM.

Moreover, to evaluate the robustness performance of the proposed EAM, four simulation experiments (Example E, Example F, Example G, and Example H) are executed in this paper. Example E is to verify the performance of EAM when the 64 kinds of equipment contain the unknown equipment. Example F is used to verify the performance of EAM when test samples of 128 kinds of equipment contain the samples of unknown equipment. Meanwhile, Examples G and H are to test the performance of EAM when the 64 kinds of equipment and the 128 kinds of equipment severally contain the attacked equipment.

As shown in Figure 7, the authentication accuracy, the FP rate, and the FN rate for Examples E and F are displayed. Moreover, when the equipment is attacked, the authentication results are displayed in Figure 8. Based on the results in Figures 7 and 8, it can be seen that the proposed EAM can well mitigate the effects of uncertainty to obtain the satisfactory robustness and accuracy. Moreover, to show the detailed performance comparing with other methods, the average values of 50 trials are used as the final results in Table 5.

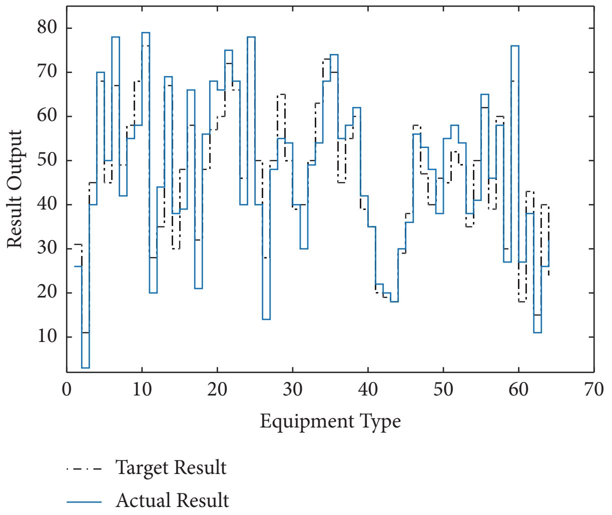


Figure 2: The identification results of EIM in Example A.

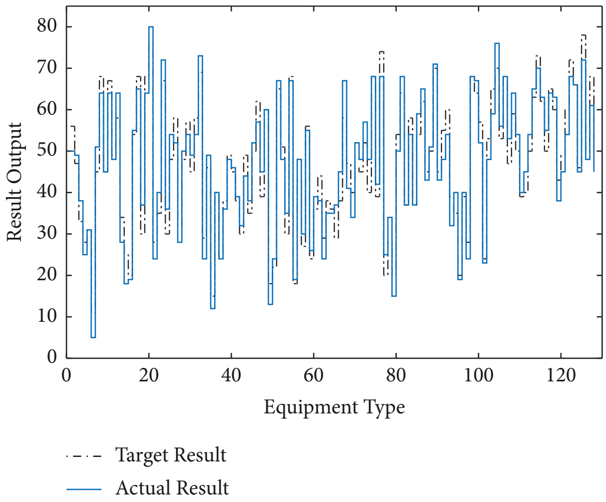


Figure 4: The identification results of EIM in Example B.

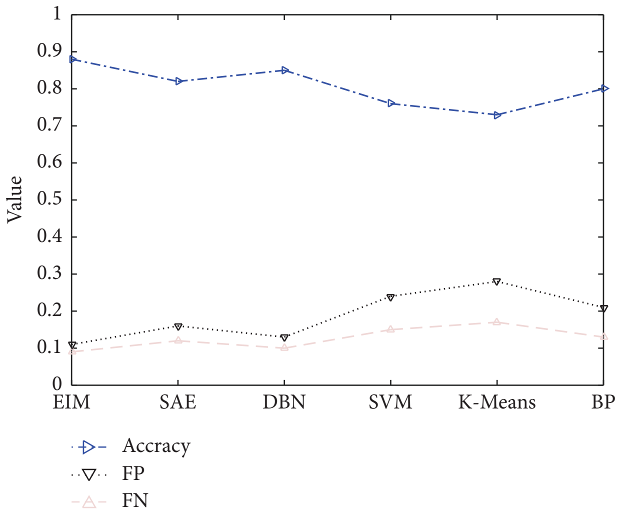


Figure 3: The identification performance of EIM in Example A.

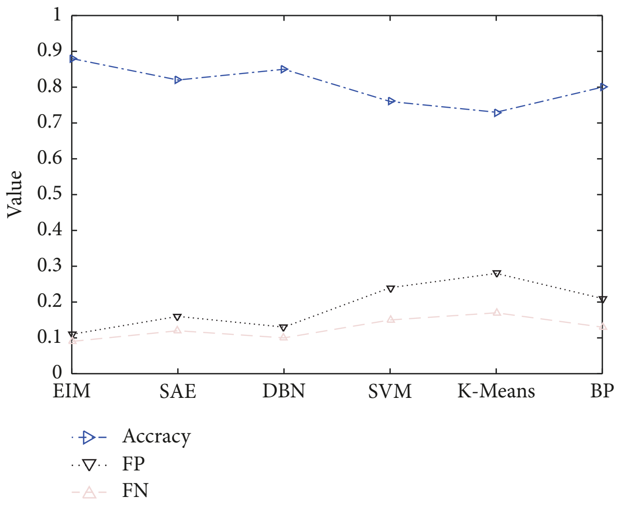


Figure 5: The identification performance of EIM in Example B.

Table 3: The comparison of identification performance of multiple methods in Example A.

Method	EIM	SAE	DBN	SVM	*k*-means	BP network
Accuracy	0.88	0.82	0.85	0.76	0.73	0.80
FP	0.11	0.16	0.13	0.28	0.28	0.21
FN	0.09	0.12	0.10	0.17	0.17	0.13

Table 4: The comparison of identification performance of multiple methods in Example B.

Method	EIM	SAE	DBN	SVM	*k*-means	BP network
Accuracy	0.84	0.8	0.81	0.7	0.69	0.72
FP	0.12	0.17	0.19	0.26	0.30	0.25
FN	0.10	0.12	0.14	0.19	0.25	0.16

According to the results of in Table 5, it can be seen that in Examples C and D, the accuracy of the proposed EAM is 0.94 and 0.92, respectively, which improves the at least 6 percentage points comparing with the accuracy of EIM. The reason of the accuracy improvement is that the EAM can avoid the authentication failure due to the error of the EIM. Meanwhile, the accuracy of EAM is 0.93, and increases the 10 percentage points more than result of EIM in Example E. And the accuracy of EAM is 0.90 and increases the 9 percentage points more than the result of EIM in Example F. Moreover, the proposed EAM has the lowest the FP rate (0.08 and 0.12) and FN rate (0.01 and 0.04) in all methods, when the testing samples are mixed into the unknown equipment in Examples E and F. In Examples G and H, the proposed EAM also has the best performance in all methods. Therefore, based on the above analysis, the proposed EAM can well weaken the uncertainty to further improve the certification performance, which can meet the requirements of equipment certification in actual production operation. Moreover, comparing with the current some hot research on device fingerprint authentication technology [37, 38], the proposed authentication method in this paper is easier to

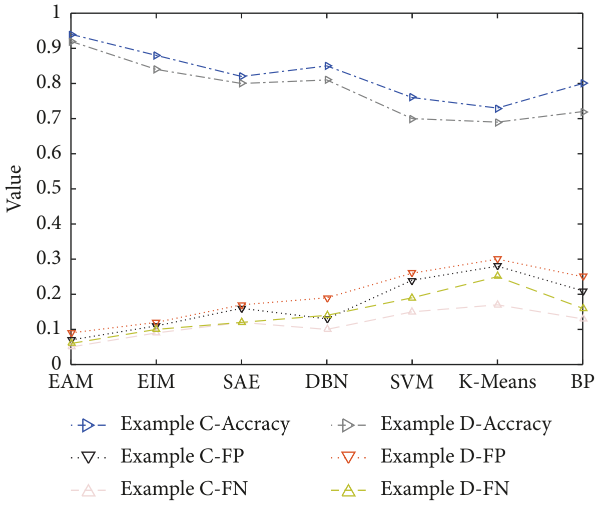


FIGURE 6: The comparison of multiple methods in Examples C and D.

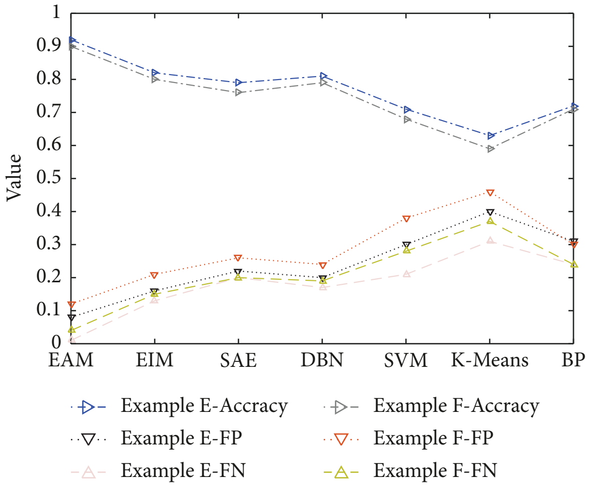


FIGURE 7: The comparison of multiple methods in Examples E and F.

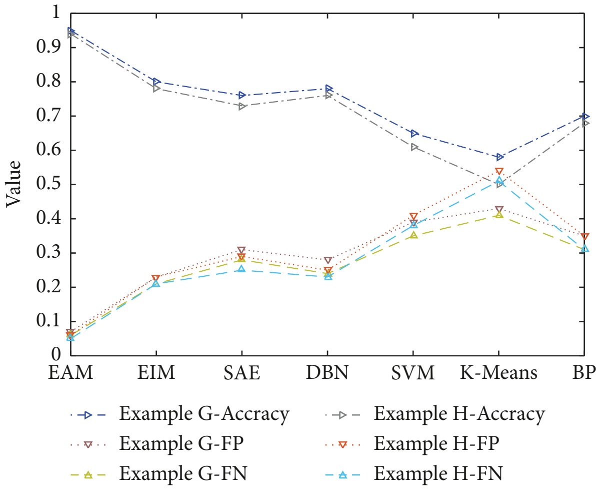


FIGURE 8: The comparison of multiple methods in Examples G and H.

apply in practice, although the accuracy is slightly inferior. In our future research, more research will be conducted to improve our approach to achieve better application effects.

4. Practical Application of Hierarchical Authentication System

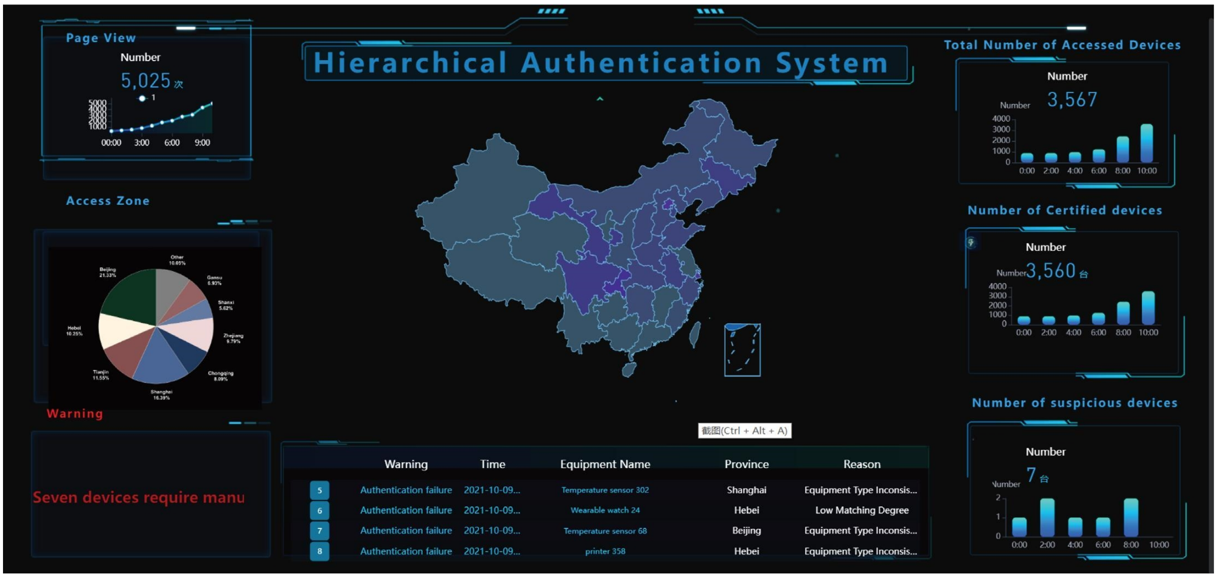
In this section, the performance and effectiveness of the proposed hierarchical authentication system are investigated in the real access platform. In this access platform, the authentication of equipment identity depends on the manual sampling, which needs a lot of manpower, and meanwhile will cause a huge safety risk for the access platform. Therefore, the hierarchical authentication system is used to recognize the equipment identity. The device authentication interface is shown in Figure 9.

As shown in Figure 9, the number of visitors is displayed in the top left of the screen, and the number of access equipment is displayed in the top right of the screen. Meanwhile, the number of the devices which are successfully authenticated and the number of devices which fail to be authenticated are shown in the right column. Moreover, for the authentication failure devices, the warning information will be prominently displayed at the bottom of the screen. The maps and pie chart can provide the regional distribution of equipment. In addition, seven devices in more than 3500 devices cannot pass the certification in Figure 10. The detailed information can view the equipment log (shown in Figure 11).

As shown in Figure 11, the log includes the time, equipment name, equipment type, province, and authentication failure reason. For example, the authentication failure reason of wearable watch 24 is the low matching degree, and the authentication failure reason of smoke transducer 54 is the change of equipment type. Based on the above analysis, the proposed hierarchical authentication system can effectively weaken the uncertainties of the IoT environment and realize the identification of the identity validity of access equipment.

Table 5: The certification comparison of multiple methods.

Examples	Index	EAM	EIM	SAE	DBN	SVM	k-means	BP network
C-64 devices	Accuracy	0.94	0.88	0.82	0.85	0.76	0.73	0.80
	FP	0.07	0.11	0.16	0.13	0.24	0.28	0.21
	FN	0.05	0.09	0.12	0.10	0.15	0.17	0.13
D-128 devices	Accuracy	0.92	0.84	0.80	0.81	0.70	0.69	0.72
	FP	0.09	0.12	0.17	0.19	0.26	0.30	0.25
	FN	0.06	0.10	0.12	0.14	0.19	0.25	0.16
E-64 devices with unknown device	Accuracy	0.93	0.82	0.79	0.81	0.71	0.63	0.72
	FP	0.08	0.16	0.22	0.20	0.30	0.40	0.31
	FN	0.01	0.13	0.20	0.17	0.21	0.31	0.24
F-128 devices with unknown device	Accuracy	0.90	0.81	0.76	0.79	0.68	0.59	0.71
	FP	0.12	0.21	0.26	0.24	0.38	0.46	0.31
	FN	0.04	0.15	0.20	0.19	0.28	0.37	0.24
G-64 devices with attacked device	Accuracy	0.95	0.8	0.76	0.78	0.65	0.58	0.7
	FP	0.07	0.23	0.31	0.28	0.39	0.43	0.35
	FN	0.06	0.21	0.28	0.24	0.35	0.41	0.31
H-128 devices with attacked device	Accuracy	0.94	0.78	0.73	0.76	0.61	0.50	0.68
	FP	0.06	0.23	0.29	0.25	0.41	0.54	0.39
	FN	0.05	0.21	0.25	0.23	0.38	0.51	0.33



Seven devices require manu

	Warning	Time	Equipment Name	Province	Reason
5	Authentication failure	2021-10-09...	Temperature sensor 302	Shanghai	Equipment Type Inconsis...
6	Authentication failure	2021-10-09...	Wearable watch 24	Hebei	Low Matching Degree
7	Authentication failure	2021-10-09...	Temperature sensor 68	Beijing	Equipment Type Inconsis...
8	Authentication failure	2021-10-09...	printer 358	Hebei	Equipment Type Inconsis...

Figure 9: The real- time authentication interface of hierarchical authentication system.

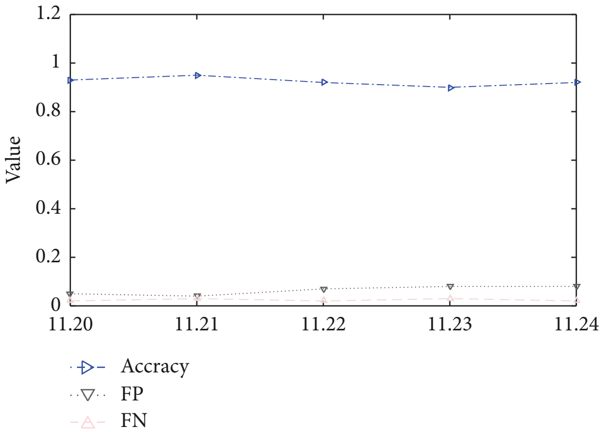
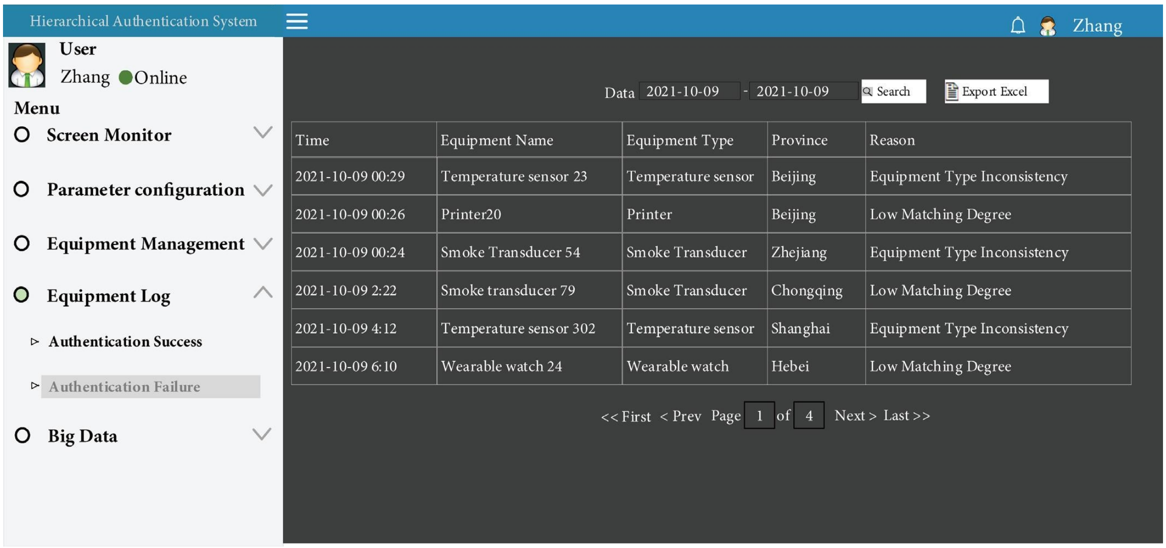


Figure 10: The authentication results in different days for access platform.



Data 2021-10-09 - 2021-10-09

Time	Equipment Name	Equipment Type	Province	Reason
2021-10-09 00:29	Temperature sensor 23	Temperature sensor	Beijing	Equipment Type Inconsistency
2021-10-09 00:26	Printer20	Printer	Beijing	Low Matching Degree
2021-10-09 00:24	Smoke Transducer 54	Smoke Transducer	Zhejiang	Equipment Type Inconsistency
2021-10-09 2:22	Smoke transducer 79	Smoke Transducer	Chongqing	Low Matching Degree
2021-10-09 4:12	Temperature sensor 302	Temperature sensor	Shanghai	Equipment Type Inconsistency
2021-10-09 6:10	Wearable watch 24	Wearable watch	Hebei	Low Matching Degree

FIGURE 11: The authentication log of hierarchical authentication system.

To demonstrate the performance of the proposed hierarchical authentication system in the real access platform, the authentication results were collected between the 20th and the 24th November. The effectiveness of five days is shown in Figure 10. It can be seen that the accuracy of this hierarchical authentication system is close to 90% with the minimal FN rate, which can be meet the actual demand.

5. Conclusion

In this paper, a hierarchical authentication system was proposed to weaken the uncertainty of the network environment to verify the validity of equipment. In this hierarchical authentication system, an EIM can be used to weaken the uncertainties of the IoT environment to effectively recognize the equipment type. Then, an EAM can further improve the robustness to obtain the satisfactory verification accuracy. Finally, the proposed hierarchical authentication system was applied into an access platform. The results demonstrated that this hierarchical authentication system can obtain good robustness and high accuracy to authenticate the identity of the access equipment. In our future work, this proposed hierarchical authentication system will be used into other cloud platforms to achieve the recognition of equipment identity.

Data Availability

Data are owned by a third party. The data underlying this paper were provided by the third party under licence/by permission. The data are shared on request to the corresponding author with permission of the third party.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Research and Development of Core Technologies in the Field of Security (grant R221006L) and Research on the Strategy of Information Technology Application Innovation grant (R22100XA).

References

[1] A. Boulaalam, “Internet of things: new classification model of intelligence,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 7, pp. 2731–2744, 2019.

[2] Z. Y. Han, L. Zhou, C. Ge, J. Li, and Z. Liu, “Robust privacy-preserving federated learning framework for IoT devices,” *International Journal of Intelligent Systems*, vol. 37, no. 11, pp. 9655–9673, 2022.

[3] D. Vergnaud, “Comment on “efficient and secure outsourcing scheme for RSA decryption in internet of things”,” *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11327–11329, 2020.

[4] K. L. Ang and J. K. P. Seng, “Application specific internet of things (ASIoTs): taxonomy, applications, use case and future directions,” *IEEE Access*, vol. 7, pp. 56577–56590, 2019.

[5] K. R. Choo, S. Gritzalis, and J. H. Park, “Cryptographic solutions for industrial internet-of-things: research challenges and opportunities,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567–3569, 2018.

[6] I. Ahmed, M. Anisetti, and G. Jeon, “An IoT-based human detection system for complex industrial environment with deep learning architectures and transfer learning,” *International Journal of Intelligent Systems*, vol. 37, no. 12, pp. 10249–10267, 2022.

[7] G. Zhong, K. Xiong, Z. Zhong, and B. Ai, “Internet of things for high-speed railways,” *Intelligent and Converged Networks*, vol. 2, no. 2, pp. 115–132, 2021.

[8] I. Ahmed, Y. L. Zhang, and G. Jeon, “A novel Internet of Things based fall detection system in smart home,” *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 9211-9212, 2019.

[9] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: an exhaustive survey on

IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[10] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[11] G. Fragkos, C. Minwalla, J. Plusquellic, and E. E. Tsiropoulou, "Artificially intelligent electronic money," *IEEE Consumer Electronics Magazine*, vol. 10, 2020.

[12] C. Tremlet and S. E. Jones, *Systems and methods for authentication based on physically unclonable functions*, vol. 5, pp. 363–375, 2017.

[13] Y. S. Yang, S. H. Lee, W. C. Chen, C. S. Yang, Y. M. Huang, and T. W. Hou, "TTAS: trusted token authentication service of securing SCADA network in energy management system for industrial internet of things," *Sensors*, vol. 21, no. 8, pp. 2685–2696, 2021.

[14] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.

[15] A. Badhib, S. Alshehri, and A. Cherif, "A robust device-to-device continuous authentication protocol for the internet of things," *IEEE Access*, vol. 9, pp. 124768–124792, 2021.

[16] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in lTE-A networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[17] K. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, 2016.

[18] D. Basin, C. Cremers, T. H. Kim, A. Perrig, R. Sasse, and P. Szalachowski, "Design, analysis, and implementation of ARPKI: an attack-resilient public-key infrastructure," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 3, pp. 393–408, 2018.

[19] A. Alrawais, A. Alhothaily, X. Cheng, C. Hu, and J. Yu, "Secureguard: a certificate validation system in public key infrastructure," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5399–5408, 2018.

[20] S. Misra, S. Goswami, C. Taneja, A. Mukherjee, and M. S. Obaidat, "A PKI adapted model for secure information dissemination in industrial control and automation 6LoWPANs," *IEEE Access*, vol. 3, pp. 875–889, 2015.

[21] O. Ruan, Y. Zhang, M. Zhang, J. Zhou, and L. Harn, "After-the-fact leakage-resilient identity-based authenticated Key Exchange," *IEEE Systems Journal*, vol. 12, no. 2, pp. 2017–2026, 2018.

[22] L. Quan, C. Zheng, and Z. Zude, "Research on secure buyer-seller watermarking protocol," *Journal of Systems Engineering and Electronics*, vol. 19, no. 2, pp. 370–376, 2008.

[23] J. Yu, V. Cheval, and M. Ryan, "DTKI: a new formalized PKI with verifiable trusted parties," *The Computer Journal*, vol. 59, no. 11, pp. 1695–1713, 2016.

[24] R. Behnia, M. O. Ozmen, and A. A. Yavuz, "Lattice-based public key searchable encryption from experimental perspectives," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1269–1282, 2020.

[25] S. Kakei, Y. Shiraishi, M. Mohri, T. Nakamura, M. Hashimoto, and S. Saito, "Cross-certification towards distributed authentication infrastructure: a case of hyperledger fabric," *IEEE Access*, vol. 8, pp. 135742–135757, 2020.

[26] L. Cao, Y. Liu, and S. Cao, "An authentication protocol in LTE-WLAN heterogeneous converged network based on certificateless signcryption scheme with identity privacy protection," *IEEE Access*, vol. 7, pp. 139001–139012, 2019.

[27] B. Chen, S. Qiao, J. Zhao et al., "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10248–10263, 2021.

[28] S. Singh, P. K. Sharma, and J. H. Park, "SH-SecNet: an enhanced secure network architecture for the diagnosis of security threats in a smart home," *Sustainability*, vol. 9, no. 4, pp. 513–527, 2017.

[29] Y. C. Wang, "Simulation of fingerprint matching identity authentication in wireless local area network," *Computer Simulation*, vol. 7, pp. 244–249, 2017.

[30] S. D. Kamvar and M. T. Schlosser, "The eigentrust algorithm for reputation management in P2P networks," in *Proceedings of the 12th international conference on World Wide Web*, New York, NY, USA, May 2003.

[31] I. Griswold-Steiner, R. Matovu, and A. Serwadda, "Wearables-driven freeform handwriting authentication," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 3, pp. 152–164, 2019.

[32] J. Seto, Y. Wang, and X. Lin, "User-habit-oriented authentication model: toward secure, user-friendly authentication for mobile devices," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 107–118, 2015.

[33] S. Vhaduri and C. Poellabauer, "Multi-modal biometric-based implicit authentication of wearable device users," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3116–3125, 2019.

[34] Q. Lin, H. J. Dai, and D. W. Ren, "A quantitative trust assessment method based on bayesian network," *Compute & Technology and development*, vol. 26, no. 12, pp. 132–1369, 2019.

[35] D. Chen and M. Z. Zhou, "Access control system based on cross-layer behaviour trust in internet of things," *Journal of Chinese Computer Systems*, vol. 37, no. 9, pp. 56–78, 2018.

[36] H. G. Han, H. J. Zhang, and J. F. Qiao, "Robust deep neural network using fuzzy denoising autoencoder," *International Journal of Fuzzy Systems*, vol. 22, no. 4, pp. 1356–1375, 2020.

[37] L. Kang, L. Zhang, X. Huang, W. Hu, and X. Yang, "Hardware fingerprint authentication in optical networks assisted by anomaly detection," *IEEE Photonics Technology Letters*, vol. 34, no. 19, pp. 1030–1033, 2022.

[38] Y. Chen, J. Pan, D. Yu, Y. Ma, and Y. Yang, "Retransmission-Based TCP fingerprints for fine-grain IoV edge device identification," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7835–7847, 2022.