Identity Authentication Technology in Edge Computing Environment: Vision and Challenges

Yuanyuan Peng[1], Sule Ye[2], Tao Qin[3(✉)], and Meng Li[4]

[1] Beijing Commsat Technology Development Co., LTD, Beijing 100000, China
[2] University of Science and Technology Beijing, Beijing 100083, China
[3] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100000, China
qintao@cert.org.cn
[4] Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract. In the era of the Internet of Everything, the number of terminal devices connected to the network is increasing day by day, and the amount of data at the edge of the network has increased dramatically. Under this background, network applications have put forward higher requirements on network bandwidth and network delay. The centralized cloud computing model can no longer meet network requirements. Edge computing emerged as a supplement and extension of cloud computing. To ensure the security of edge computing communications, efficient and reliable identity authentication technology is particularly important. To this end, first introduced the generation of edge computing, and at the same time analyzed and elaborated several major identity authentication technologies, combined with the demand characteristics of edge computing, analyzed the development direction of identity authentication technology in the edge computing environment.

Keywords: Edge computing · Security requirements · Identity authentication

1 Introduction

Cisco predicts that the future will be the era of the Internet of Things technology. With the rapid development of the Internet of Things technology and its widespread application in the field of actual production and life, the number of network terminals has also increased dramatically. This application trend has brought about a sharp increase in the amount of data generated by the terminal. At the same time, due to the promotion of cloud services, the cloud computing paradigm is not enough to cope with the problems facing the network now [1]. Therefore, to supplement cloud computing, the concept of edge computing is proposed.

In recent years, edge computing has attracted more and more investment and research interest in the industry. In early 2013, Nokia and IBM jointly launched a cloud server for radio applications, which is an edge computing platform for 4G/LTE networks. In 2014, the standardization of mobile edge computing started under the auspices of the European Telecommunications Standards Institute (ETSI) [2]. In June 2015, Vodafone, Intel,

X. Sun et al. (Eds.): ICAIS 2021, CCIS 1423, pp. 606–613, 2021.
https://doi.org/10.1007/978-3-030-78618-2_50

Huawei and Carnegie Mellon University jointly launched the Open Edge Computing Initiative (OEC). In October 2016, the first IEEE/ACM Edge Computing Workshop was held in Washington, DC. Today, edge computing plays a central role in the upcoming 5G technology.

However, edge computing faces many key issues in practical applications. The primary condition for the successful implementation of edge computing is security. In the edge computing paradigm, the network edge is in a highly dynamic and heterogeneous complex environment, which leads to extremely difficult network security protection, which brings new network security challenges [3–7].

In an edge computing environment, edge servers, cloud servers, and users play the roles of providing services and accessing resources, respectively, and are in different trusted domains. The low latency requirements of edge computing and the mobility of end users make identity authentication a difficulty. In the process of edge computing communication, it is necessary to make sure that the identity of each communication object is true and effective, which is of great significance to the security of edge computing.

2 Secure Key Technology for Edge Computing

So far, in order to solve the identity authentication in the communication process in the edge computing environment, researchers have proposed many related technologies.

2.1 Identity Authentication Technology Based on Cryptography

The two parties involved in the authentication confirm the identity of the other party by sending encrypted information about the identity. The method of encrypting the message may use symmetric encryption technology or asymmetric encryption technology. The author uses symmetric encryption technology to encrypt the message, and combines the Hash function to verify the authenticity of the other party's identity during the challenge response, and finally realizes the two-way identity authentication of the fog server and fog user [8, 9]. On the basis of [8], a virtual ID is established for the edge user, which achieves the goal of anonymous authentication and reduces the risk of user privacy leakage during the authentication process. The security of cryptography mainly relies on reliable key distribution, management and maintenance mechanisms. This feature leads to the limitation of its application performance in the wireless transmission environment under dynamic movement and the edge computing scenarios with limited resources [10]. In general, if you want the encryption algorithm to be more secure, the key size should be larger, but it requires a larger key storage space. Therefore, terminals with limited resources cannot meet the key storage requirements of traditional complex encryption algorithms.

2.2 Identity Authentication Scheme Based on Biometrics

For each biological individual, it has unique, stable and reliable biometrics. The biometric-based identity authentication scheme uses biometrics as the identification, and combines image analysis technology and pattern recognition technology to identify

and identify the authentication object Identity, more common face recognition, fingerprint recognition and voice verification. In the literature, Liu Shuhua and others used Kinect cameras to obtain RGB and infrared radiation images of human faces, and used multi-task cascaded convolutional networks to crop and align the collected images. Next, the processed data was used to train the CNN model for activity detection. The FaceNet model is trained with RGB images for face recognition, and finally an anti-spoofing identity authentication scheme based on face recognition is realized [11]. P. Punithavathi et al. Proposed a lightweight cloud-based cancelable biometric authentication system framework. They used random projection transformation technology to convert the obtained fingerprint into multiple templates, and then performed authentication based on Euclidean distance The template matching operation between objects completes the identity authentication process. In this scheme, the converted template is used to replace the real fingerprint information, which has the effect of being replaceable and anonymous [12]. Although the biometrics-based identity authentication scheme has high reliability, it requires a large amount of calculation and requires a large amount of memory to store biometric data. At the same time, this scheme requires expensive and precise identification equipment, which does not meet the requirements of edge computing Low-cost, low-power application requirements.

2.3 Password-Based Identity Authentication Scheme

Both parties in identity authentication agree and store a private password in advance. When authentication is required, the user submits the password and the other party checks it to complete the identity authentication. Password authentication is simple and easy to implement, but the security is weak, and it is easy to be cracked by exhaustive attacks and dictionary attacks.

The method of hash chain is abandoned, and the two-way password authentication is realized with a single hash function. This authentication algorithm is more flexible and reduces the amount of calculation [13]. In addition to traditional text passwords, there are graphic passwords. In modern people's lives, touch screen technology is widely used in smart terminals. By randomly changing the position of the digital graphic on the touch screen, the user can draw different graphic unlocking procedures according to the unique or backup PIN password each time. This method makes it more complicated and more difficult for an attacker to steal user information, thereby increasing the user Information security [14].

2.4 Identity Authentication Scheme Based on Physical Layer

This is a new type of identity authentication technology in recent years, which is different from other traditional identity verification methods to ensure secure communication within the network. This scheme uses physical signals or hardware characteristics of the device to identify the identity.The two types of physical layer attributes used for device authentication are mainly composed of the mutual channel characteristics of wireless transceivers and some analog front end (AFE) defects [15]. Aiming at the asymmetric resource edge computing system, a physical layer identity authentication scheme based on clustering is proposed in [5]. This scheme combines lightweight cryptography

technology and CSI based physical layer authentication technology to realize two-way identity authentication between edge devices and terminals. Confirm the identity of the other party by analyzing the statistical characteristics of the channel state information (CSI) [16]. Run-Fa Liao et al. Proposed a deep learning-based physical layer authentication framework for industrial wireless sensor networks [17], they obtain CSI and preprocess the data to form a training data set, and use the training data and corresponding tags to train the deep neural network (DNN), convolutional neural network (CNN) and convolutional preprocessing neural network (CPNN). Get a deep learning model. In the identity authentication stage, CSI is used as the input of the model, and the output is the identity authentication result. The physical layer-based authentication scheme has the irreplaceable advantages of other traditional methods. The specific physical layer characteristics are directly affected by the equipment and environment during the communication process, and it is difficult for an attacker to simulate counterfeiting. However, the instability of fast time-varying channels often reduces the performance of physical layer authentication. In addition, the performance of AFE defect-based authentication technology is limited by the low reliability of AFE defect estimation [18].

In recent years, deep learning [19] has received many effective improvements and demonstrated its good application performance. Therefore, it has received widespread attention from researchers in various fields. The application of machine learning and deep learning algorithms to identity authentication schemes has become a kind of trend. In [20], the author proposes a physical layer identity authentication scheme based on CSI, which uses a convolutional neural network to extract a set of features that are stable with respect to rotation from the original CSI measurement data, and then compares the user's previous CSI with the CSI received by the heart To determine whether the user's identity is legal and valid. This scheme can achieve the effect of identity authentication, but because every authentication must traverse all users in the system, resulting in lower authentication efficiency.

3 Development Direction of Identity Authentication Technology in Edge Computing Environment

Through the research and summary of the identity authentication technology in the edge computing environment, in order to achieve a safe and reliable identity authentication effect, in the future research, the identity authentication technology in the edge computing environment should develop in the following aspects.

3.1 Technology Migration

So far, the identity authentication technology has made many important achievements, with various authentication methods, and also has considerable effects in security. However, most of the current research on identity authentication is still focused on other computing paradigms. The research on identity authentication technology specifically for edge computing is relatively small. The characteristics of edge computing are not fully considered. The identity authentication technology that is really applicable to edge computing is still in place in the exploration stage [21].

Therefore, we can consider migrating from identity authentication schemes applied to other computing paradigms to edge computing, such as cloud computing, mobile edge computing, and fog computing. However, the technical solution cannot be applied to the edge computing environment, but the characteristics of the edge computing terminal, such as limited computing / storage resources and low latency requirements, should be considered to appropriately improve the identity authentication scheme.

Password-based identity authentication technology is often used in other computing paradigms. Among them, Kerberos [22] is a typical password authentication system, which belongs to a symmetric password system. The Kerberos authentication system uses a trusted third-party authentication scheme, and its database stores the authentication server and the user's key. Therefore, the authentication system can complete the function of authenticating the identity of another entity for one entity. However, Kerberos has the risk of the old authentication code being reused, and because its server needs to store a large number of keys, the key management problem will become an unfavorable factor restricting its best performance in edge computing. Therefore, the shortcomings of Kerberos can be improved to enhance the effectiveness and security of identity authentication in the edge computing environment. For example, in order to solve the weakness of excessive key storage, it can be combined with the public key cryptosystem, and the Kerberos system no longer needs to store keys, so that the key management problem can be solved, and the efficiency of identity authentication is also improved.

3.2 Integration of Multiple Identity Authentication Technologies

Through the analysis of multiple identity authentication technologies, it is found that these technical solutions have their advantages, but at the same time there are many shortcomings. For example, the hardware cost of identity authentication technology based on machine learning is too high, and the amount of calculation data required is too large; the identity authentication technology based on cryptography has problems such as key management, key length size, and security that are difficult to balance; in biometric authentication The collected biometric data may cause data distortion due to interference noise. On the other hand, when the research technology is applied to solve practical problems, due to environmental factors or human factors, the application effect will be poor, and the security will not meet expectations.

Considering the above reasons, multiple technologies can be organically combined to learn from each other. This identity authentication scheme is a good idea to be applied in the edge computing environment. Combining the advantages of multiple technologies can improve the reliability and reliability of edge computing identity authentication effectiveness.

As a whole, the password-based authentication method is the simplest and easy to perform, but it is easy to be attacked by attackers; the cryptography-based authentication technology is the most mature, widely used, with various solutions and stable performance; smart cards can store secret information and provide hardware encryption, High security; due to the uniqueness of biometrics, it is not easy to be forged, so the authentication technology based on biometrics is the most secure. If the advantages of these technologies can be properly combined, it can make up for the shortcomings of some of

these solutions and improve the actual availability of the overall identity authentication scheme in the edge computing environment.

For example, the most common thing today is to combine biometric authentication with deep learning. Chaoran Liu et al. Adopted the fusion feature of local binary mode and oriented gradient histogram, and used unsupervised convolution constraint Boltzmann machine to train the gait energy map, and proposed a kind of input from gait energy map to gait recognition the result of the program. This algorithm framework that integrates deep learning into gait recognition can obtain efficient gait recognition results based on a small amount of gait images, which improves the efficiency and accuracy of recognition [23].

3.3 Unified Identity Authentication Mechanism

With the continuous development of edge computing, there are more and more edge computing applications. When a user needs to access edge computing resources, the user needs to perform multiple identity authentication operations, and the data containing private information will be repeatedly input during multiple identity authentication, which will bring huge privacy risks to users. In addition, the edge server needs to create a large number of user databases, so managing and maintaining the database will be an extremely complex and difficult problem. Considering these factors, it is very important to study a unified identity authentication technology suitable for edge computing.

In the edge computing environment, the identity management between different edge servers can be regarded as authentication between different trust domains. If a unified identity authentication method is used for resource access requests, users can achieve cross-platform through only one identity authentication, Cross-domain operations.

There are many well-known unified identity authentications at present, For example, IBM's WebSphere solution [24], Net Passport developed by Microsoft [25].

Zhang Fuyou and others proposed a unified identity authentication scheme based on biometrics. When the user performs a single sign-on operation, the scheme can simultaneously provide users with security and convenience through the biometrics identification device of the mobile terminal device and the trusted environment Authentication function. When users request access to the service, they will use their biometrics instead of user names and passwords to pass identity authentication, so users do not need to frequently input messages containing private information, and the risk of user privacy leakage will be significantly reduced [26].

4 Conclusions

Edge computing occupies a core position in the rapidly developing Internet of Things technology and has broad practical application prospects. However, edge computing also faces many new security challenges. Efficient and reliable identity authentication is an important way to solve security problems, which can greatly reduce the risk of user privacy leakage. According to the characteristics of edge computing with low latency and limited terminal resources, research on lightweight identity authentication technology is the main challenge. At the same time, in order to better explore the identity authentication

technology that is highly suitable for edge computing, it is a research direction worthy of attention to migrate from other computing paradigms to develop identity authentication technology; faced with the advantages and disadvantages of many different identity authentication technologies, many The concept of technology fusion has certain practical significance; with the increasing use of edge computing, unified identity authentication technology is an inevitable development trend. In general, how to form an identity authentication technology that truly meets the needs of edge computing needs in-depth research.

Acknowledgement. This work is supported by the National Natural Science Foundation of China under Grant (No. 61971032), Fundamesntal Research Funds for the Central Universities (No. FRF-TP-18-008A3).

Conflicts of Interest. The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. IBM and Nokia Siemens Networks Announce World's First Mobile Edge Computing Platform #MWC13, Press Release, Nokia, 25 February 2013. company.nokia.com/en/news/press-releases/2013/02/25/ibm-and-nokia-siemens-networks-announce-worlds-frst-mobile-edge-computing-platform-mwc13
2. Antipolis, S.: ETSI announces first meeting of new standardization group on mobile-edge computing, The Standard, European Telecommu-nications Standards Inst., 30 October 2014. www.etsi.org/news-events/news/838-2014-10-news-etsi-announces-first-meeting-of-new-standardization-group-on-mobile-edge-computing
3. Li, H., Zhou, C., Haitao, X., Lv, X., Han, Z.: Joint optimization strategy of computation offloading and resource allocation in multi-access edge computing environment. IEEE Trans. Veh. Technol. **69**(9), 10214–10226 (2020)
4. Hong, X., Wang, Y.: Edge computing technology: development and countermeasures. Strateg. Study Chin. Acad. Eng. **20**(2), 20–26 (2018)
5. Rodrigues, T.G., Suto, K., Nishiyama, H., et al.: Hybrid method for minimizing service delay in edge cloud computing through VM migration and transmission power control. IEEE Trans. Comput. **66**(5), 810–819 (2017)
6. Shi, W., Sun, H., Cao, J., et al.: Edge computing: a new computing model in the era of internet of everything. Comput. Res. Dev. **1** (2017)
7. Varghese, B., Wang, N., Barbhuiya, S., et al.: Challenges and opportunities in edge computing. In: 2016 IEEE International Conference on Smart Cloud (SmartCloud), pp. 20–26. IEEE (2016)
8. Ibrahim, M.H.: Octopus: an edge-fog mutual authentication scheme. IJ Netw. Secur. **18**(6), 1089–1101 (2016)
9. Amor, A.B., Abid, M., Meddeb, A.: A privacy-preserving authentication scheme in an edge-fog environment. In: IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), pp. 1225–1231. IEEE (2017)
10. Liu, H., Wang, Y., Liu, J., et al.: Practical user authentication leveraging channel state information (CSI). In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, pp. 389–400 (2014)

11. Liu, S., Song, Y., Zhang, M., et al.: An identity authentication method combining liveness detection and face recognition. Sensors **19**(21), 4733 (2019)
12. Punithavathi, P., Geetha, S., Karuppiah, M., et al.: A lightweight machine learning-based authentication framework for smart IoT devices. Inf. Sci. **484**, 255–268 (2019)
13. Ling, C.H., Lee, C.C., Yang, C.C., et al.: A secure and efficient one-time password authentication scheme for WSN. IJ Netw. Secur. **19**(2), 177–181 (2017)
14. Shen, S.S., Kang, T.H., Lin, S.H., et al.: Random graphic user password authentication scheme in mobile devices. In: 2017 International Conference on Applied System Innovation (ICASI), pp. 1251–1254. IEEE (2017)
15. Zeng, K., Govindan, K., Mohapatra, P.: Non-cryptographic authentication and identification in wireless networks. Netw. Secur. **1,** 3 (2010)
16. Chen, Y., Wen, H., Wu, J., et al.: Clustering based physical-layer authentication in edge computing systems with asymmetric resources. Sensors **19**(8), 1926 (2019)
17. Liao, R.F., Wen, H., Wu, J., et al.: Deep-learning-based physical layer authentication for industrial wireless sensor networks. Sensors **19**(11), 2440 (2019)
18. Wang, X., Hao, P., Hanzo, L.: Physical-layer authentication for wireless security enhancement: current challenges and future developments. IEEE Commun. Mag. **54**(6), 152–158 (2016)
19. Pouyanfar, S., Sadiq, S., Yan, Y., et al.: A survey on deep learning: algorithms, techniques, and applications. ACM Comput. Surv. (CSUR) **51**(5), 92 (2019)
20. Yazdani Abyaneh, A., Pourahmadi, V., Hosein Gharari Foumani, A.: CSI-based authentication: extracting stable features using deep neural networks. Trans. Emerg. Telecommun. Technol. **31**(2), e3795 (2020)
21. Zhang, J., Zhao, Y., Chen, B., Hu, F., Zhu, K.: Survey on data security and privacy-preserving for the research of edge computing. J. Commun. **39**(3), 1–21 (2018)
22. Neuman, B.C., Ts'o, T.: Kerberos: an authentication service for computer networks. IEEE Commun. Mag. **32**(9), 33–38 (2002)
23. Liu, C., Wq, Y.: Gait recognition using deep learning. In: Handbook of Research on Multimedia. Cyber Security (2020)
24. Camargo, C., Martens, H.: IBM Websphere Portal 8: Web Experience Factory and the Cloud. Packt Publishing (2012)
25. Deng, Y., Cheng, X.H.: System design of mobile cross-domain single sign-on. Comput. Eng. Des. **31**(8), 1667–1672 (2010)
26. Fuyou, Z., Wang, Q., Song, L.: Research on unified identity authentication system based on biometric recognition. Inf. Netw. Secur. (09), 86–90 (2019)