Identity Authentication Under Internet of Everything Based on Edge Computing

Zixiao Kong[1(✉)], Jingfeng Xue[1], Yong Wang[1], Weijie Han[1,2], and Xinyu Liu[3]

[1] School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China
bit_kzx2017@126.com
[2] Space Engineering University, Beijing 101416, China
[3] The Experimental High School Attached to Beijing Normal University, Beijing 100081, China

Abstract. With the rapid development of the Internet, the application of the Internet of things and big data is more and more extensive. The era of Internet of everything (IoE) has come, and the traditional cloud computing model has been unable to efficiently process the massive data generated by a large number of edge devices. Therefore, edge-type big data processing which is oriented to massive data computing generated by network edge devices—edge computing comes into being. However, due to the complexity of edge computing, data security and privacy issues become more prominent. Aiming at the security authentication of edge equipment under the Internet of everything, this paper designs an identity authentication framework under the Internet of everything based on edge computing. In the framework, multi-factor identity authentication is applied to solve the weakness of edge equipment security authentication. Moreover, the software defined network technology (SDN) is adopted to realize the global management of the deployment and application of a large number of edge equipment, which can effectively realize the effective security protection of the Internet of everything. In the end, the formalized verification of the identity authentication process of the designed framework is carried out.

Keywords: Edge computing · Internet of everything · Identity authentication · SDN

1 Introduction

With the rapid development of Internet and Internet of things technology, online entity identity has been growing at an explosive pace. Nowadays society is changing from the industrial civilization to the information civilization, and to the intelligent development. A digital, networked, intelligent and cloud-based Internet of everything era is coming. As early as 2005, cloud computing has quietly changed our life, work and study. As for cloud computing platform of the rapid development of Internet of things, the number of sensors, smart phones, wearable devices, smart home appliances and other devices increases linearly. What follows is the massive amount of data generated by IOT terminals [1]. According to the cisco global cloud index [2], by 2019, 45% of the data

W. Han et al. (Eds.): CTCIS 2019, CCIS 1149, pp. 72–85, 2020.
https://doi.org/10.1007/978-981-15-3418-8_6

generated by the Internet of things will be stored, processed and analyzed on the edge of the network. The total data traffic of the global data center is expected to reach 10.4 ZB. By 2020, the global data center traffic will reach 15.3 ZB [3]. At the same time, the number of IOT devices connected has also shown a linear growth trend in recent years. According to the Internet business solutions group, the number of wireless devices connected to the network will reach 50 billion by 2020 [4]. In this case, traditional cloud computing cannot meet the demand of Internet of everything (Fig. 1), and edge computing comes into being.

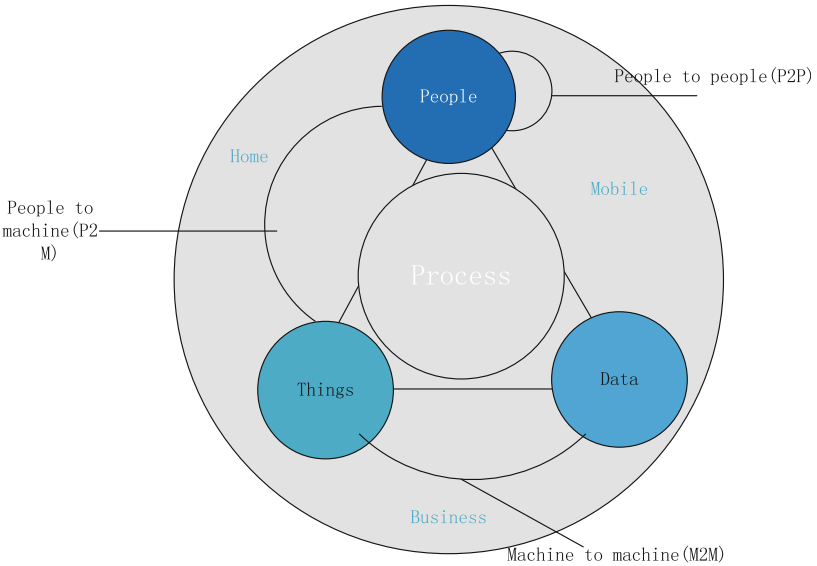

Fig. 1. Internet of Everything.

Edge contains applications, data calculation, network and equipment of four domains, which usually contain more than one function entity, such as data participants (the end user, infrastructure providers and service providers), service (virtual machine, data containers) and infrastructure (edge data centers, terminal infrastructure and core infrastructure) (Fig. 2) [5]. In this kind of multi-entity edge computing system, the demand of users' cross-domain networking increases rapidly. As a result, identity authentication faces huge challenges [6].

The main contributions of this paper include:

(1) presenting cloud computing, edge computing, SDN and other concepts to readers in different fields, and making a reasonable explanation of identity authentication based on edge computing instead of cloud computing under the IoE;
(2) combine SDN with edge computing model to give full play to the advantages of SDN;
(3) an identity authentication architecture based on edge computing under the IoE is proposed, which adopts multi-factor identity authentication with high security level.

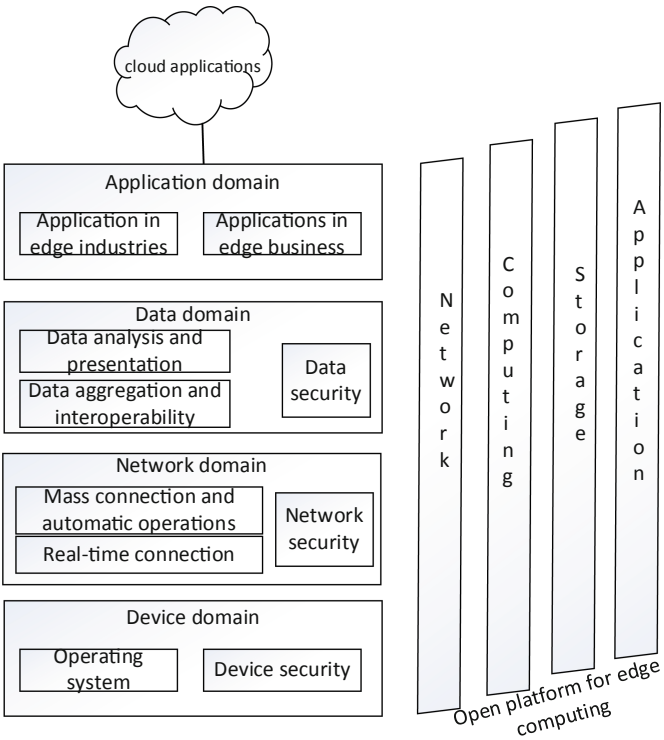

Fig. 2. Edge computing reference architecture.

2 Related Work

Identity authentication is an eternal war in the field of network security [7]. At present, identity authentication is mainly carried out on the basis of cloud computing platform. The information technology represented by cloud computing has profoundly changed people's way of production, work, study and life. This way of identity authentication is characterized by stable network, cost saving and high flexibility [8].

Bangui et al. proposed a transfer of services from a centralized cloud platform to a distributed platform. Edge computing is cited in the case. The integrated edge cloud computing brings many advantages, such as reducing network delay, dynamic flexibility, etc. However, there are still some network deficiencies in edge computing [9].

Liu et al. proposed an attribute based ciphertext access control optimization method for mobile cloud. The fusion of mobile Internet and cloud computing reduces the cost, has high reliability and is dynamic and extensible. Although the length of communication ciphertext increases in the process of data release, it is completely acceptable in the real environment [10].

Roy et al. proposed a mobile cloud computing security lightweight user authentication scheme based on encrypted graphics hash, bit XOR and fuzzy extraction function. ProVerif 1.93 simulation verifies that the authentication scheme has lower

calculation cost and communication cost compared with relevant schemes, but it is more suitable for users of low-power computing devices [11].

Badr et al. proposed a technology to encrypt and share important medical data through cloud computing. Through this system, the decryption process is delegated to the cloud server to achieve scalability and low computational complexity on the data owner side, ensuring speed. Each cloud facilitates cost savings for users, and security challenges faced by cloud entities are addressed and addressed. In the cloud computing environment, data access has controlled access and access control permissions of multiple user roles, which realizes secure and confidential access to data [12].

Jin et al. designed a homomorphic encrypted communication protocol based on RLWE for user authentication and message management in the internet-of-things fusion environment based on cloud computing. By analyzing the performance of the existing Internet of things environment communication protocol and the proposed communication protocol, the security of the protocol is verified. Using the data in the cloud computing environment management server and the Internet of things in the environment of gateway between fully homomorphic encryption algorithm, designed the data validation techniques, is higher than traditional encryption algorithm efficiency and safety. In data leakage, infringement of user information and other vulnerabilities will continue to deepen [13].

Dhillon et al. proposed a multi-factor ECC authentication scheme for medical service security based on cloud Internet of things. This scheme uses the web-based AVISPA tool for formal analysis and verifies that the scheme is safe against both active and passive attacks, including replay attack and man-in-the-middle attack. Compared with the performance of the relevant scheme, the calculation cost of the scheme is lower. Nevertheless, there is still room for improvement in real-time heterogeneity and complexity [14].

Most of the solutions are cloud computing models under the Internet of things, and some of the solutions using edge computing models have shortcomings in the network surface. Considering the above reasons, this paper combines edge computing with SDN to make the network more flexible and dynamic and provide more efficient authentication.

3 Preliminaries

With the further development of IoE and the integration of IoE, many emerging industries will surely be derived [15]. The IoE will create new functions for enterprises, individuals and countries, and bring new experiences and development opportunities. At the same time, it also brings many challenges [16].

Computing is transitioning from single-user devices to the IoE. The IoE combines people, processes, data and things together. Cloud computing mostly adopts a centralized management method, which makes cloud services create high economic benefits. In the context of the Internet of Everything, application services require low latency, high reliability, and data security. The traditional cloud computing model (Fig. 3) can no longer efficiently process the massive data generated under the Internet of everything [17]. The main reasons are as follows [18]:

(1) Cloud computing is unable to handle the massive data with explosive growth. At present, big data processing has entered the era of edge computing centered on the IoE from the era of centralized processing centered on cloud computing. In the era of centralized big data processing, more is to centrally store and process big data. The approach taken is to build a cloud computing center and leverage the cloud computing center's superior computing power to centrally solve computing and storage problems. In contrast, in the era of edged big data processing, network edge devices generate massive amounts of real-time data. Moreover, these edge devices will deploy an edge computing platform that supports real-time data processing to provide users with a large number of services or functional interfaces, and users can call these interfaces to obtain the required edge computing services.
(2) Network transmission bandwidth load increases, leading to network delay. In the Internet of Everything environment, edge devices generate a large amount of real-time data, and cloud computing performance is gradually reaching a bottleneck. According to the Internet Data Center, by 2020, the total amount of global data will be greater than 40ZB. As the amount of data on edge devices increases, network bandwidth is becoming another bottleneck in cloud computing. Increasing network bandwidth alone does not meet the latency requirements of emerging Internet of Everything applications. For this purpose, performing some or all of the calculations on edge devices close to the data source is an emerging computing model that adapts to the needs of the Internet of Everything application.
(3) Marginal data involves personal privacy, which requires improved security protection. When users use e-shopping websites, search engines, social networks and so on, the users' private data will be uploaded to the cloud center. With the popularity of smart homes, many families install webcams in their homes. If video data is directly uploaded to the cloud data center, the transmission of video data not only occupies bandwidth resources, but also increases the risk of revealing user privacy data. To this end, for the data security problem of the existing cloud computing model, the edge computing model provides a better privacy protection mechanism for such sensitive data. On the one hand, before the user's source data is uploaded to the cloud data center, the data source is directly processed by the edge node of the near data end to implement protection and isolation of some sensitive data; on the other hand, the edge node establishes a functional interface with the cloud data, that is, the edge node only receives the request from the cloud computing center and feeds back the result of the processing to the cloud computing center, which can significantly reduce the risk of privacy leakage.
(4) Energy consumption of data transmission. As more and more user applications run in cloud computing centers, the demand for energy consumption in large-scale data centers will be difficult to meet in the future. To solve this energy consumption problem, the edge computing model proposes to decompose some computing tasks running on the original cloud data center, and then transfer the decomposed computing tasks to the edge nodes for processing. In this way, the computing load of the cloud computing data center is reduced, thereby achieving the purpose of reducing energy consumption.

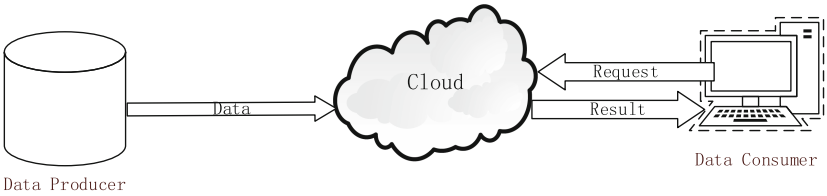

Fig. 3. Traditional cloud computing models.

Currently, the linear growth of centralized cloud computing capabilities has been unable to match the explosive growth of massive edge data. A single computing resource based on cloud computing model can no longer meet the requirements of real-time, security and low energy consumption of big data processing. On the basis of the existing cloud computing model, the edge computing model emerges at the right moment. They complement each other and are applied to the processing of big data at the cloud center and edge to solve the problem of insufficient cloud computing services in the era of Internet of Everything. Edge computing refers to an open platform that integrates the core functions of network, computing, storage and application [19]. The edge computing model is shown in Fig. 4. Under the edge computing model, the main data processor is the edge device, and the cloud server is more used as the receiver of processing results. Therefore, the risk of privacy data exposure is effectively reduced [20].

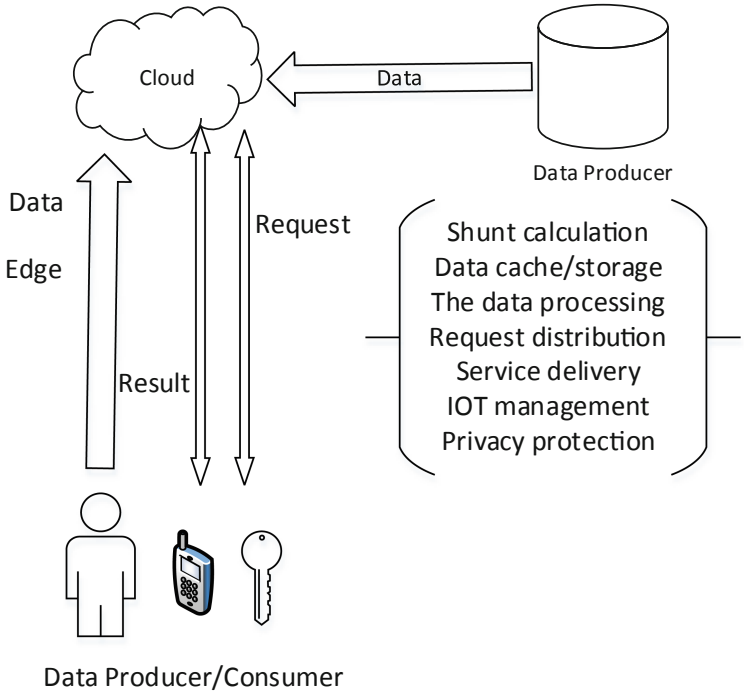

Fig. 4. Edge computing model.

With the rapid development of global network and communication, the traditional network has exposed many shortcomings: unclear division of service traffic, insufficient horizontal expansion ability, too large broadcasting domain, inability to quickly launch computing resources, and excessive network delay [21]. In 2008, clean slate research group of Stanford university proposed software defined network architecture (Fig. 5), which improved the shortcomings of traditional network [22]. SDN architecture has three layers: application layer, control layer and infrastructure layer. The SDN controller collects network topologies, calculates routes, creates and transfers flow tables, and manages and controls networks. Infrastructure devices only transmit traffic and execute policies. The normalized northern interface provides the required resources and services for the upper applications.

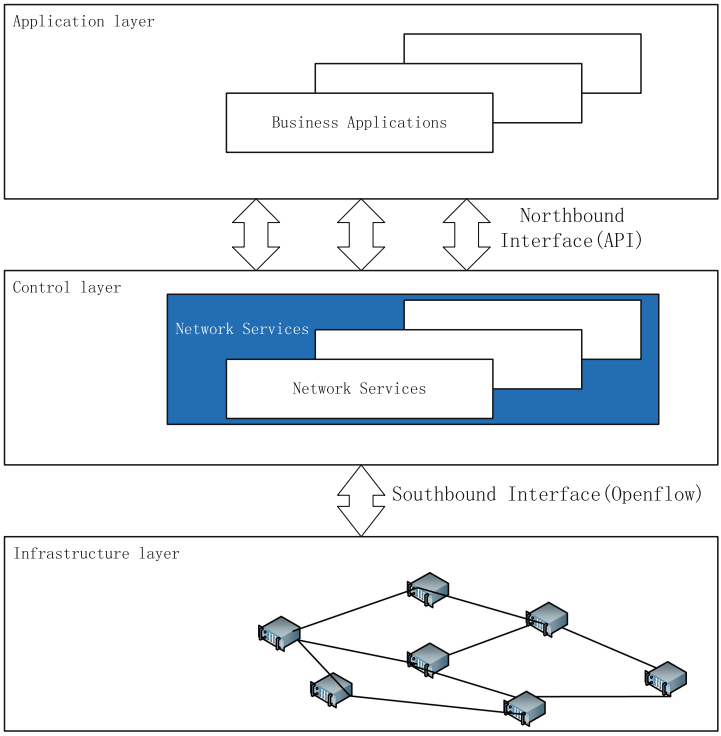

Fig. 5. SDN architecture.

4 Design of Framework

For identity authentication in Internet of everything based on edge computing, currently deployed technologies cannot provide efficient access control specification or authentication in traditional networks. In the framework of SDN, control plane and data plane are separated [23]. Administrators have the flexibility to control network traffic through centralized controllers without having to access physical devices. Centralized

optimization of network resources, improve efficiency, simplify management, accelerate network innovation, shorten the start-up cycle of new functions [24].

This paper proposes a frame of reference to apply multi-factor identity authentication and SDN to edge computing [25]. Edge computing coordinator uses the nature of network management of SDN to conduct service discovery and choreography requirements of edge computing services. The centralized SDN controller has a global view of the network, and the edge computing coordinator can integrate with the SDN controller to collect information from the network [26]. The authentication module consists of a database server, an identity authentication server, a terminal and an application service provider. The database server stores the information of each network entity. Finally, multi-factor authentication method is used to complete the authentication, which includes password, fingerprint and digital certificate [27].

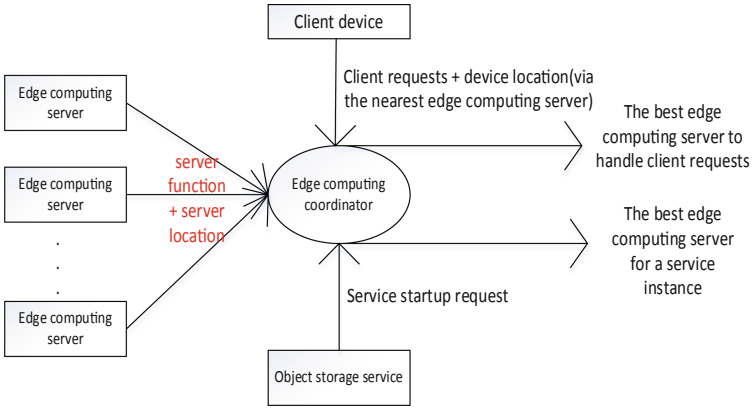

Fig. 6. Edge computing coordinator.

As shown in Fig. 6, edge computing coordinator is introduced to solve the limited computing capacity, critical latency, bandwidth and load balancing of edge computing servers. As a medium, edge computing coordinator connects applications to the right classes of edge computing servers [28].

As shown in Fig. 7, the edge computing coordinator is integrated with the SDN controller. Adding SDN can make the network more flexible and dynamic. Besides, the SDN controller can manage the edge computing coordinator northbound application, which can be programmed to handle a variety of situations. Therefore, edge computing coordinator can reuse SDN architecture. What is more, the northbound applications define the network behavior, SDN controller provides the northbound API for these applications to trigger commands. The controller also has a southbound interface (usually based on OpenFlow) that communicates with the managed device [29].

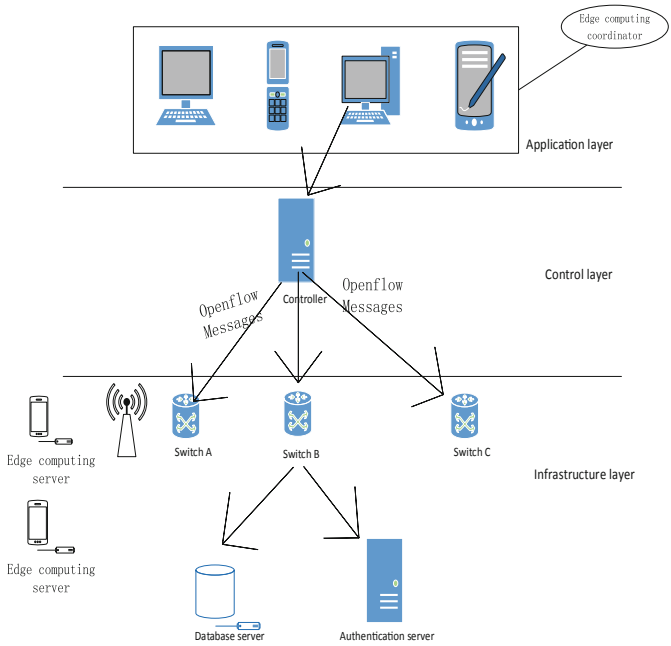

Fig. 7. Edge computing framework based on SDN.

As shown in Fig. 8, it is an identity authentication architecture based on edge computing. The authentication process is as follows:

Step 1: the end user requests access to the application;
Step 2: the application service provider requests the authentication server to verify the end user;
Step 3 and step 4: two-way authentication between the authentication server and the end user;
Step 5: the authentication server replies to the application service provider about the end user authentication results;
Step 6: the application service provider accepts or rejects the end user's request based on the authentication result of the authentication server.

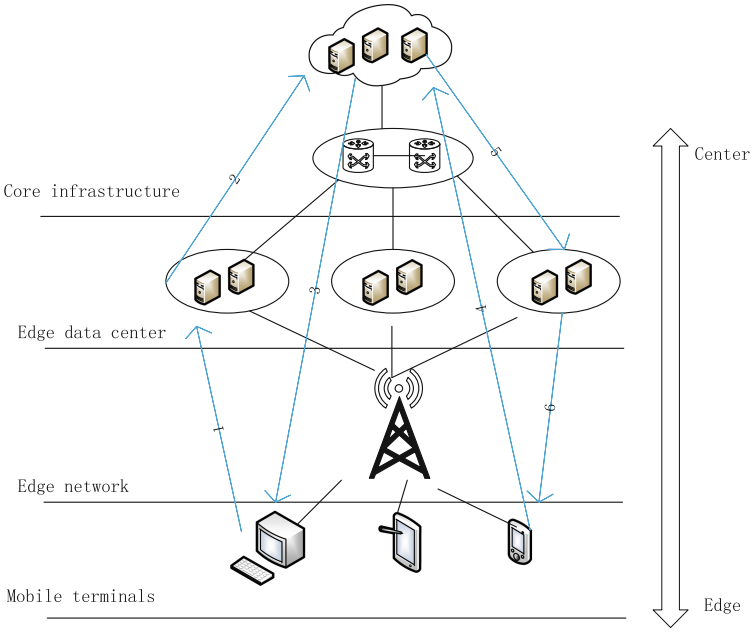

Fig. 8. Identity authentication architecture based on edge computing.

5 Formal Validation of Identity Authentication

The main authentication process is performed between the end user and the authentication server. For simplicity, only the authentication scheme between the user and the authentication server is described. Our scheme consists of the following three modules.

5.1 Registration

If an end user wants to become a valid user of secure applications on the Internet, they must register in advance. During the registration process, users should present their identity information to the authentication server for registration and apply for digital certificates from the authentication server. The main process is as follows:

(1) generate a pair of authentication server keys (SK_S, PK_S) based on the public key generation algorithm. SK_S is the private key of the verification server, and the corresponding public key is PK_S. After that, the verification server selects a robust security hash function H(·). Finally, the authentication server publishes its public key PK_S and hash function H(·) to all potential users.

(2) after obtaining the public key PK_S and hash function H(·), the user starts to register. Because fingerprint recognition is becoming more and more common, this paper adds fingerprint recognition to the authentication of users. First, after obtaining the user's fingerprint data b, the terminal calculates Gen(b) → (U,V). And let U become the user's private key SK_C, V is the public string produced

simultaneously, the corresponding public key is PK_C. Then the user sets ABC and PWD as the login username and corresponding password, and calculates M1 = E_{PKs} (ABC||PWD||PK_C||H(SK_C)). In the end, the user sends M1 through the common channel to the authentication server.

(3) after obtaining M1, the authentication server decrypts D_{SKs}(M1) = (ABC||PWD|| PK_C||H(SK_C)) with its private key SKS. Then the server verifies the legitimacy of ABC and PWD. If the authentication fails, the server will ask the user to send a new message, otherwise the server will give the digital certificate Cert = E_{PKc}(PWD|| PK_C ||PK_S||Sig_{SKs}(PWD|| PK_C ||PK_S)). Finally, the server saves ABC, H(PWD), PK_C,H(SK_C) in the database and sends Cert to the user.

(4) after obtaining the Cert, the user decrypts D_{SKc}(Cert) = PWD||PK_C||PK_S||Sig_{SKs} (PWD||PK_C||PK_S) through its private key SK_C. Then verifying the digital signature of the certificate—Sig_{SKs} (PWD|| PK_C ||PK_S), if successful, the user saves the certificate to the terminal and the registration process ends.

5.2 Verification

If a registered user wants to access the application, follow these steps:

(1) the user enters his user name ABC and password PWD in the login page.

(2) after obtaining the user name and password, the authentication server calculates H (PWD) and compares it with the information in the local database. If it is not equal, access is denied. Otherwise, go to step 3.

(3) the user enters his fingerprint on the client, using the fingerprint data b′ and the help data V stored locally, and then the client calculates Rep(b′, V) → U. The correctness of the fuzzy extractor method ensures that the string U is the user's private key SKC. The client calculates M2 = E_{PKs}(E_{SKc}(r1)), where r1 is a random number that sends the message M2 to the authentication server.

(4) after obtaining the message M2, the authentication server first encrypts it through its private key SK_S and the user's public key PK_C. Then the authentication server selects a different random number r2 and calculates M3 = E_{PKc}(H(SK_C)||r1||r2). Finally, the authentication server sends the message M3 to the client.

(5) after receiving the message M3, the client decrypts the message D_{SKc}(M3) = (H (SK_C))′||r1′ ||r2. For receiving (H(SK_C))′ and r1′, the equation (H(SK_C))′ = H (SK_C) and r1′ = r1 need to be checked. The authentication server then computes the message M4 = E_{PKs} (r2) and sends it to the authentication server.

(6) after obtaining the message M4, the authentication server decrypts the message D_{SKc} (M4) = r2′ and determines whether the equation r2′ = r2 is true. If so, the authentication server accepts that the user is a legitimate user and allows him to access the application, otherwise access will be denied.

5.3 Cancellation

If a user does not want to use his digital certificate anymore, he can ask for the certificate to be canceled, as follows:

(1) the user calculates his digital certificate cancellation request Dele = E_{PKs} (ABC‖PWD‖Sig_{SKs} (ABC ‖PWD)) and sends it to the authentication server.
(2) after obtaining Dele, the authentication server decrypts the message D_{SKc}(Dele) = ABC‖PWD ‖Sig_{SKc} (ABC‖PWD).
Signature ABC‖PWD and Sig_{SKc}(ABC‖PWD) will be verified later. If the signature cannot be verified, the cancellation request will fail. Otherwise, the authentication server changes the status of the user certificate to "cancel" by searching the records in the database of the keyword ABC. Finally, the authentication server sends the result of the cancellation request to the user.
(3) after obtaining the successful cancellation message, the client will delete the stored digital certificate, and the cancellation process is over.
Our proposed identity authentication scheme based on edge computing under the Internet of everything is multi-factor authentication. First, the account name ABC and password PWD are validated. Second, fingerprint data is validated to generate the correct private key for the end user. Finally, the end user's digital certificate is used in the interactive authentication process between the end user and the authentication server. Therefore, the proposed scheme has a high level of security and is difficult to break.

6 Conclusion

Under the Internet of everything, the traditional cloud computing model is no longer able to efficiently deal with the explosive growth of massive data, hence the emergence of the edge computing model. To solve the problem of identity authentication under the Internet of everything based on edge computing, this paper proposes a reference framework. It applies multi-factor identity authentication (including password, fingerprint and digital certificate) and software-defined network to edge computing, and formalizes the identity authentication process of the designed framework.

Acknowledgement. This work was supported by the National Key Research & Development Program of China (2016QY06X1205).

References

1. Shi, W., Sun, H., Cao, J., et al.: Edge computing: a new computing model in the Internet of everything era. Comput. Res. Dev. **54**(5), 907–924 (2017)
2. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper, 01 February 2018. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html
3. Cisco cloud index supplement. Cloud readiness regional details white paper (2017)
4. Evans, D.: The Internet of everything: how more relevant and valuable connections will change the world. Cisco IBSG **2012**, 1–9 (2012)
5. Zhang, J., Zhao, Y., Chen, B., Hu, F., Zhu, K.: Research review on edge computing data security and privacy protection. J. Commun. **39**(03), 1–21 (2008)

6. An, X., Cao, G., Miao, L., Ren, S., Lin, F.: Security review of intelligent edge computing. Telecommun. Sci. **34**(07), 135–147 (2018)
7. Han, W., Xue, J., Wang, Y., Liu, Z., Kong, Z.: MalInsight: a systematic profiling based malware detection framework. J. Netw. Comput. Appl. (125), 236–250 (2019). ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.10.022
8. Han, W., Xue, J., Wang, Y., Huang, L., Kong, Z., Mao, L.: MalDAE: detecting and explaining malware based on correlation and fusion of static and dynamic characteristics. Comput. Secur. (83), 208–233 (2019). ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.02.007
9. Bangui, H., Rakrak, S., Raghay, S., et al.: Moving to the edge-cloud-of-things: recent advances and future research directions. Electronics **7**, 309 (2018)
10. Liu, J., Ming, M., Wang, H., et al.: Optimization method of attribute-based ciphertext access control for mobile cloud. J. Commun. **39**(373) (7), 43–53 (2018)
11. Roy, S., Chatterjee, S., Das, A.K., et al.: On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services. IEEE Access **5**, 25808–25825 (2017)
12. Badr, A.M., Zhang, Y., Gulfam, H., Umar, A.: Dual authentication-based encryption with a delegation system to protect medical data in cloud computing. Electronics **8**, 171 (2019). https://doi.org/10.3390/electronics8020171
13. Jin, B.W., Park, J.O., Mun, H.J.: A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment. Wirel. Pers. Commun. **105**, 599–618 (2018)
14. Dhillon, P.K., Kalra, S.: Multi-factor user authentication scheme for IoT-based healthcare services. J. Reliab. Intell. Environ. **4**(3), 141–160 (2018)
15. Zhang, X., Shao, Y., Sun, C.: Overall design of smart transportation for future cities. Urban Transp. (05), 1–7 (2018)
16. Mei, H.: Everything can be connected and everything can be programmed. Fangyuan (12), 58–59 (2018)
17. Liu, J., Xiao, Y., Chen, C.L.P.: Authentication and access control in the internet of things. In: International Conference on Distributed Computing Systems Workshops. IEEE Computer Society (2012)
18. He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., Ur, B.: Rethinking access control and authentication for the home internet of things (IoT). In: Proceedings of USENIX Security Symposium (2018)
19. Tu, Y., Dong, Z., Yang, H.: Key technologies and application of edge computing. ZTE Commun. **15**(02), 26–34 (2017)
20. Wang, F., Wen, H., Chen, S., Chen, L., Hou, W.: Protection method of mobile intelligent terminal privacy data under edge computing. Cyberspace Secur. **9**(02), 47–50 (2018)
21. Chen, Z., Guo, B., Zhang, Y.: MEC technology scheme and application analysis of 5G network edge computing. Mob. Commun. **42**(07), 34–38 (2018)
22. Qin, H., Liu, L.: Research on decentralized SDN access identity authentication. Appl. Comput. Syst. **27**(9), 243–248 (2018). http://www.c-s-a.org.cn/1003-3254/6509.html
23. Xu, F., Ye, H., Cui, S., Zhao, C., Yao, H.: Software defined industrial network architecture for edge computing offloading [J/OL]. J. China Univ. Posts Telecommun. 1–9 (2018). https://doi.org/10.19682/j.cnki.1005-8885.2018.0030
24. Tian, Y., Zhang, N., Lin, Y.-H., Wang, X., Ur, B., Guo, X., Tague, P.: SmartAuth: user-centered authorization for the internet of things. In: Proceedings of the USENIX Security Symposium (2017)

25. Wang, M.: A three-factor two-way identity authentication scheme in mobile internet. In: Proceedings of 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017), Research Institute of Management Science and Industrial Engineering: Computer Science and Electronic Technology International Society, p. 5 (2017)
26. He, W., et al.: Rethinking access control and authentication for the home internet of things (IoT). In: Proceedings of the USENIX Security Symposium (2018)
27. Dong, H., Zhang, H., Li, Z., Liu, H.: Computational unloading of service workflow in mobile edge computing environment [J/OL]. Comput. Eng. Appl. 1–12 (2018). http://kns.cnki.net/kcms/detail/11.2127.TP.20181101.1416.033.html
28. Zhao, Y., Zhang, X.: New media identity authentication and traffic optimization in 5G network. In: 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 1331–1334 (2017)
29. Fan, X., Lu, Z., Ju, L.: Security of SDN southbound channel. J. Beijing Univ. Electron. Sci. Technol. **24**(04), 15–20 (2016)