Journal of Computers Vol. 32 No. 4, 2021, pp. 179-186
doi:10.53106/199115992021083204014

# Design and Implementation of Cloud-Edge Integrated Security Authentication System

Cai-sen Chen[1], Bo-gong Ji[2*], Ying-zhan Kou[1], Jia-xing Du[2]

[1] Center of Exercise and Training, Army Academy of Armored Forces, Beijing, 100072, China

[2] Department of Information and Communication Army Academy of Armored Forces, Beijing, 100072, China
caisenchen@163.com, 13910133595@139.com, kyzh0323@sina.com, dhtl2004@163.com

Received 1 June 2021; Revised 1 July 2021; Accepted 2 August 2021

Abstract. With the rapid development and widespread application of the Internet of Things, big data, and 5G networks, traditional cloud computing cannot handle the massive amounts of data generated by network edge devices. Therefore, edge computing has emerged. With the addition of edge nodes, the traditional cloud architecture has gradually evolved to a "cloud-edge" integrated architecture. This new network architecture brings convenience and new challenges to network security. Due to the open features of edge computing, such as content perception, real-time computing, and parallel processing, the existing security authentication problems in the cloud computing environment have become more prominent. Based on the analysis of the particularity of the existing cloud-edge computing environment, this paper proposes the basic architecture of the cloud-side integrated security authentication system, and analyzes the availability and security of the architecture.

Keywords: cloud edge integration, edge computing, safety certificate, SM2 algorithm

## 1 Introduction

With the rapid development of Internet of Things technology and 5G network architecture, new service models continue to emerge, such as intelligent transportation, smart cities, location services, and mobile payments. The number of smart phones, wearable devices, networked TVs and other sensing devices will show an explosive growth trend, followed by "massive" data generated by IoT terminals [1]. As more and more smart devices generate massive amounts of information during the operation, corresponding computing power and network bandwidth are required to ensure the normal provision of services [2].

The traditional cloud computing model cannot meet the application requirements of the Internet of Everything. The perception layer data of the Internet of Things is at a massive level [3], and there are frequent conflicts and cooperation between the data, which has strong redundancy, correlation, real-time and multi-source heterogeneous characteristics. Converged multi-source heterogeneous data and real-time processing requirements have brought huge challenges to cloud computing that cannot be solved [4]. Cloud service is a kind of centralized service computing with a high degree of aggregation. Users send data to the cloud for storage and processing, which will consume a lot of network bandwidth and computing resources. At the same time, a large number of user visits will also increase network traffic [5], which will cause service interruption and network delays. In addition, the network edge devices in the Internet of Everything mode usually have limited resources [6], and the problem of long-distance transmission of data between the edge devices and the cloud computing center is particularly prominent. Besides, the traditional cloud computing model needs to upload these private data to the cloud computing center, which will increase the risk of leaking users' private data. In particular, in delay-sensitive application environments such as industrial sites, when millions of smart devices request services, the current cloud computing architecture is difficult to meet the needs of smart devices for mobile support, location awareness, and low latency [7]. This gives rise to a model of data processing at the edge, known

* Corresponding Author

as edge computing.

As a new computing model, edge computing is a distributed computing infrastructure that uses one or more IoT devices or edge devices close to the user side to perform a large amount of communication, control, storage, and management [8]. Through the connection between edge devices and terminal devices, on the one hand, the processing burden of resource-constrained devices is reduced, and on the other hand, localized processing provides lower latency and reduces the amount of data transmitted by the core network.

Edge computing is not intended to replace cloud computing, but as a supplement to cloud computing, to provide better services for IoT users through edge-cloud collaboration. In the edge computing environment, the traditional cloud architecture has evolved into a "cloud-edge" integrated architecture. Identity authentication is the first step for devices to access the network. Edge devices need to authenticate their identity to the cloud and provide other access terminals authentication service. The terminals in the edge computing environment are massive, mobile, complex, and multiple security domains coexist. New features make the existing identity authentication protocol in the cloud computing environment no longer applicable [9].

At present, most of the research on the edge computing environment focuses on the application aspect, while the research on the security aspect is less. Therefore, it is of great significance to study the security authentication mechanism in the cloud side environment in this paper. Based on the in-depth analysis of the security issues faced by the Internet of Things identity authentication in the edge computing environment, this paper studies the architecture of the "cloud-edge" integrated security authentication system suitable for the edge computing environment. In this framework, based on the SM2 encryption algorithm, a "cloud-edge" integrated security authentication scheme based on identity is further designed. This scheme realizes the efficient access authentication of edge devices in edge computing environment [10]. Then we analyze the security and feasibility of the certification scheme.

## 2 Related Work

Aiming at the identity authentication problem of the Internet of Things in the edge computing environment, the current research mainly focuses on the cloud computing architecture. Sarvabhatla et al. proposed an authentication method based on user biometric fingerprints [11]. This method is applied to wireless sensor networks and requires users to register biometric information with the cloud center before accessing the network. The server verifies the user's identity through the combination of biometric information and password. This method requires a centralized authentication server, which cannot meet the authentication requirements of terminal mobility in the edge computing environment. Ali Zeeshan et al studied the security certification scheme of fog calculation [12] which is vulnerable to clogging attacks, However, the authentication scheme is not considered in the cloud edge system. For the cloud security or intrusion detection system (IDS) an effective scheme for prediction and privacy preservation is employed with the use of enhanced Honeypot algorithm [13] that considers security solutions only from a cloud perspective. Chu F et al. proposed an authentication scheme based on the ECC algorithm [14]. All ECC public parameters are calculated by the base station in the initialization phase, and the sensor public key and private key are generated according to the calculated parameters. Echeverria S et al. proposed a trusted identity solution based on secure key generation and exchange, which is used for edge device authentication and trusted identity establishment in a disconnected environment, but this method is expensive. And as the network grows, nodes need more storage space [15]. Donald et al. defined a centralized infrastructure for mobile edge computing, using a single trusted third party as an authentication server [16]. This method requires the authentication server to be accessible at all times. The edge environment is relative to the cloud center environment. It is more complicated and the network is prone to interruptions, so the applicability of this scheme is limited. Tsai et al. [17] realize the authentication of edge terminals and edge devices based on public key cryptography and security hardware, and can realize offline authentication, but this scheme requires all devices to store certain credential information of all users in the trust domain. And it is not suitable for multi-trust domain environment. Wu Kehe et al. designed a secure authentication scheme based on SM2 in the Internet of Things system [18], but did not consider the realization of unified identity authentication on the cloud edge system.

In summary, although the security issues of the Internet of Things in the edge computing environment

have attracted more and more attention, most of the researches have analyzed the existing security threats at a relatively high level and failed to propose corresponding solutions [19]. In addition, the existing research focused on the edge and terminal side, using the computing power of edge devices to perform some complex operations for IoT terminals, but failed to study unified security authentication issues in the edge computing environment under the "cloud-edge" integrated network architecture. Therefore, there is an urgent need for a cloud-edge integrated security authentication scheme suitable for edge computing to provide security protection for the development of edge computing. This is the focus and main contribution of this paper.

## 3 System Model

In this part, we first introduced the identity authentication technology, including the relevant content of the national secret SM2 identification password algorithm. Then the basic architecture of the cloud-edge integrated security authentication system is proposed, and finally we propose the specific cloud-edge integrated system security authentication scheme.

### 3.1 Identity Authentication Technology

SM2 is the national secret standard elliptic curve encryption algorithm, and the elliptic curve multiple point operation forms a one-way function. In the calculation of multiple points, the problem of knowing the multiple point and the base point to solve the multiple is called the elliptic curve discrete logarithm problem. For the discrete logarithm problem of general elliptic curve, there are only exponential computational complexity solutions at present. Compared with the large number decomposition problem and the discrete logarithm problem on finite fields, the solution of the elliptic curve discrete logarithm problem is much more difficult. Therefore, under the same security requirements, elliptic curve ciphers require much smaller key sizes than other public key ciphers.

In the digital signature algorithm, a signer generates a digital signature on the data, and a verifier verifies the authenticity of the signature. Each signer has a public key and a private key, where the private key is used to generate the signature, and the verifier verifies the signature with the signer's public key. Before the signature generation process, use the cryptographic hash algorithm to compress; before the verification process, use the cryptographic hash algorithm to compress the information in the same way.

SM2 digital signature algorithm includes three parts: key generation, signature generation and signature verification.

**a. Key generation**

(1) Randomly select key $d$, $d \in [1, q-1]$;

(2) Calculate $P = dG$ and publish $P$ as a public key and save $d$ as a private key;

G is the base point of order $q$ in an elliptic curve.

**b. Signature generation**

(3) The signer selects a random number $k \in [1, q-1]$ and calculates $kG = (x_1, y_1)$;

(4) Calculate $r = Hash(m) + x_1 \bmod q$, where $m$ is the message to be signed, and Hash is a one-way hash function; if $r = 0$ or $r + k = q$, re-select the random number $k$.

(5) Calculate; if $s = 0$, re-select the random number $k$; otherwise, use $r$, $s$ as the sig $s = (1+d)^{-1}$ $(k - rd) \bmod q$ nature result.

**c. Signature verification**

(6) After the verifier receives $m$ and $r$, $s$, it first checks whether satisfies $r, s \in [1, q-1]$ and; then calculates $(x_1^1, y_1^1) = sG + (r+s)P$

(7) Calculate $r^1 = Hash(m) + x_1^1 \bmod q$; judge whether $r$ and $r^1$ are equal, if they are equal, the signature verification passes, otherwise the verification fails.

## 3.2 Cloud Edge Integrated Security Authentication System

### 3.2.1 Basic Architecture

As a new computing model, edge computing migrates part of the computing tasks of cloud computing to the local area to realize localized services for IoT terminals. Changes in network architecture also make the traditional authentication model no longer applicable. In the edge computing environment, the edge device needs to complete identity authentication to the cloud when accessing the network and the cloud allocates some local services to it. Users only need to authenticate their identity to the edge device, without directly sending an authentication request to the cloud. Combining the characteristics of the edge computing environment, the "cloud-edge" integrated authentication architecture proposed in this paper is shown in Fig. 1.

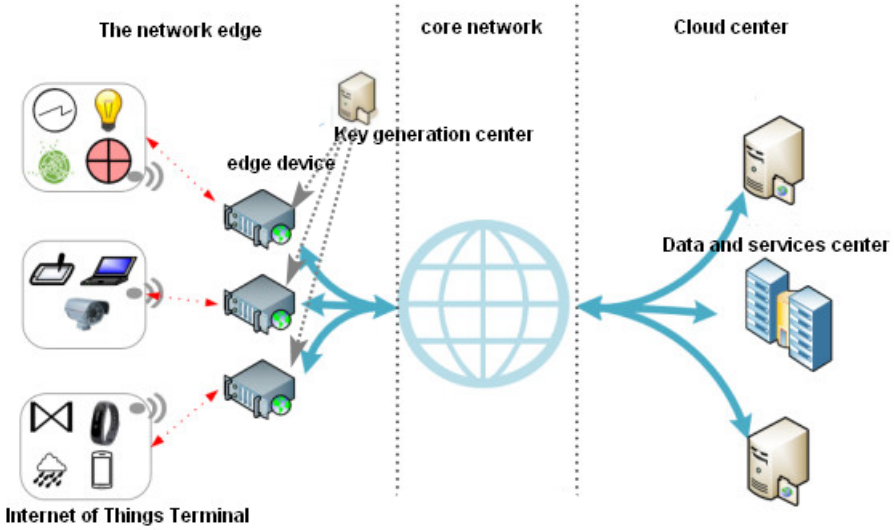


**Fig. 1.** Cloud edge integrated architecture

The cloud center is mainly used to provide Internet of Things services, solve the global distribution of some policy data, manage edge node and receive data uploaded by the lower-level Internet of Everything devices for analysis and processing, and provides authentication access services for edge devices; edge devices are deployed on the user side which provides edge intelligent services for the terminal device, and the deployment of the edge device can be flexibly deployed according to the size of the specific network.

PKI (Public Key Infrastructure) provides a complete set of security infrastructure for network applications, it maps the terminal and the public key, and enables other terminals to verify the mapping relationship. As a mature authentication technology, PKI builds the security foundation of the Internet world. However, there will be many problems when terminals and edge devices, as well as edge devices and the cloud all use PKI authentication mechanisms. For example, the large number of IoT terminals puts great pressure on the maintenance and storage of certificates and the backup and recovery of user key pairs; the certificate verification process is expensive, which is not suitable for resource-constrained IoT devices; IoT devices are more vulnerable to disruption because they are in an open environment, and frequent joining and exiting the network will also pose more challenges to the CA's certificate revocation list update.

The cryptographic algorithm based on SM2 identification is constructed on the basis of elliptic curve bilinear pairing, which can generate a public-private key pair with the identification as the public key according to the identity of the terminal, and realize the identification-based digital verification signature, data encryption and decryption, key exchange and other functions. Compared with the PKI system, the identity-based cryptographic algorithm does not require the CA to generate a certificate for the user to ensure the credibility of the user's public key, which reduce the cost of certificate verification; at the same time, it does not require a trusted third party to save the user's key pair, reducing the complexity of key management; Identity-based passwords can easily build a private authentication system. In the entire

identity-based password system, you can quickly build a logo-based certification system only if the signature master key and encryption master key of the private key generation center is changed.

The "cloud-edge" integrated security authentication architecture shows that the entire network is mainly composed of edge devices and the cloud. When the device is initialized, the KGC will distribute the identity for the edge device and generate the corresponding public and private key pair. Each terminal has its own identity, key pair, system parameters and other information.

### 3.2.2 Safety Certification Scheme

We propose the cloud-side integrated security authentication system assuming that there is a trusted third-party key generation center (KGC), which is mainly responsible for registering and maintaining the public key of each node. When the edge device joins the system, it first submits the public key and other necessary information to KGC for signing up. The security authentication algorithm of this scheme is constructed based on the SM2 digital signature algorithm. Therefore, it is similar to the SM2 digital signature algorithm, including 4 steps of system initialization, key generation, signature generation, and signature verification, as follows.

(1) System initialization

First select a large prime number $p$ greater than 160 bits, and then select one elliptic curve $y = x^3 + ax + b$ (a and b are selected elliptic curve parameters, meet $4a^3 + 27b^2 \neq 0 \ mod \ p$ ), choose the base point (generator) $G$ with order $n$ . Choose a secure symmetric encryption algorithm, such as SM4, for the convenience of description, this scheme is abbreviated as $E$, and the corresponding encryption algorithm is $D$. Choose a safe hash function, such as SM3, abbreviated as $H$.

(2) Key generation

Edge device A randomly chooses $d_A \in [1, n-1]$ as its private key and calculates its public Key $P_A = d_A G = (x_A, y_A)$. Every edge device must sign up in KGC.

The edge device A has an identifiable $ID_A$ with a bit length of $entlen_A$. It is recorded that $ENTL_A$ is 2B data converted from an integer $entlen_A$. Both the signer and the verifier need to use the cryptographic hash algorithm to obtain the hash value $Z_A$.

(3) Signature generation

Suppose the message to be signed is $m$, edge device will sign it and send it to other edge device or the cloud center. The signature of message $M$ is $\sigma = \{r, s\}$, and the edge device sends $\sigma$ to other edge device or cloud center. As shown in Table 1.

**Table 1.** Signature generation algorithm

**Algorithm 1.** Signature generation algorithm

**Input:** Initial data for edge device A (Elliptic system parameter, $Z_A$, $m$, $P_A$, $d_A$)

**Output:** Encrypt complete data $M$, digital signature($r$, $s$)

1. $\overline{M} \leftarrow Z_A \| m$
2. $e \leftarrow H_v(\overline{M})$
3. $k \leftarrow rand()\%(n-1)+1$ //Generate random number $k \in [1, n-1]$
4. $(x_1, y_1) = [k]G$ //Calculate elliptic curve point
5. $r \leftarrow (e + x_1) \bmod n$
6. if $(r = 0)$ *or* $(r + k = n)$ then
7. reselect the random number $k$ and repeat
8. else
9. $s \leftarrow ((1 + d_A)^{-1}(k - r \bullet d_A)) \bmod n$
10. if $s = 0$ then
11. reselect the random number $k$ and repeat
12. else
13. return ($r$, $s$)
14. end
15. end

(4) Signature verification

After the authentication object receives the signature information, it calculates the relevant parameters and judges whether *R* and *r'* are equal. If they are equal, the signature is received, and the edge device is authenticated to perform data encryption transmission communication and related service licenses. As shown in Table 2.

**Table 2.** Signature verification algorithm

**Algorithm 2.** Signature verification algorithm

**Input:** Initial data for edge device (cloud center) B (Elliptic system parameter, $Z_A$, $M'$, ($r'$, $s'$))

**Output:** The digital signature verifies the results (true or false)

1. if $r'$ ϵ [1, $n$-1] and s' ϵ [1, n-1] then
2. $\overline{M}' \leftarrow Z_A \| M'$
3. $e' \leftarrow H_v(\overline{M}')$
4. $t \leftarrow (r' + s') \bmod n$
5. if $t = 0$ then
6. return false
7. else
8. $(x_1', y_1') = [s']G + [t]P_A$ // Calculate elliptic curve point
9. $R = (e' + x_1') \bmod n$
10. if $R = r$' then
11. return false
12. else
13. return true //Digital signature validation successful
14. end
15. end
16. else
17. return false
18. end

## 4 Scheme Assessment

### 4.1 Feasibility

This signature scheme is constructed based on the SM2 digital signature scheme, and the SM2 digital signature scheme is implemented based on a secure elliptic curve. The elliptic curve cipher has extremely high computational efficiency. Using a 160-bit key in the elliptic curve cipher algorithm, the security strength equivalent to the 1,024-bit key in RSA can be obtained. Therefore, this scheme is lightweight and suitable for edge environments, which don't need a large number of certificates and reduce the storage pressure of edge devices.

### 4.2 Security

The communication between edge devices and the communication between edge devices and the cloud will pass through an insecure network. After adopting the security authentication based on the SM2 algorithm, the integrity and non-repudiation of the communication can be maintained. In this scheme, a secure hash function H is used. If the message *M* is damaged during the encryption process, or $C_m$ (encryption using the receiver's public key) is damaged during the signature transmission process, then the *M*' calculated by the verifier is different from *M*. According to the anti-collision principle of the hash function, the hash values obtained must be different, which will cause R and r' to be unequal, and the signature verification fails. Therefore, the integrity of this program is guaranteed. Since this scheme is constructed based on the SM2 signature scheme, this scheme can satisfy the existence and unforgeability characteristics. If an edge device tries to deny its signature σ on *M*, it is impossible for anyone except the device to forge another message m* that is different from *M*, and make its signature σ. Therefore, the user cannot deny the signature σ of *M*. According to this, this scheme realizes non-repudiation.

## 5 Conclusion

The existing cloud computing model can no longer meet the real-time requirements of massive IoT terminals. As a new computing model, edge computing deploys edge devices with computing and storage capabilities locally, and the edge devices provide services for the IoT terminals. With the addition of edge nodes, the traditional cloud architecture has gradually evolved to a "cloud-edge" integrated architecture. This new network architecture brings convenience while also bringing new challenges to IoT identity authentication and privacy protection.

Based on the in-depth study of the characteristics of the edge computing environment, this paper proposes a "cloud-edge" integrated security authentication system, and under this architecture, designs a flexible and efficient security authentication scheme suitable for the edge computing environment. Afterwards, on the basis of theoretical research, we propose a specific safety certification scheme. Finally, we analyze the feasibility and safety of the scheme which proved the value of this scheme.

## Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments. This research was supported by the National Natural Science Foundation of China under Grant No. U1836101, and Fund projects in the technical field of the basic strengthening plan of the science and Technology Commission of the Military Commission under Grant No. 2019-JCJQ-JJ-031.

## References

[1] W. Shi, H. Sun, J. Cao, Q. Zhang, W. Liu, Edge computing-an emerging computing model for the Internet of everything era, Journal of Computer Research and Development 54(5)(2017) 907-924.

[2] M. Sarvabhatla, C.S. Vorugunti, A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN, IEEE Fourth International Conference of Emerging Applications of Information Technology, 2014.

[3] Z. Ali, S.A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, Y.B. Zikria, A clogging resistant secure authentication scheme for fog computing services, Computer Networks 185(2021) 107731.

[4] A. Mondal, R.T. Goswami, Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security, Microprocessors and Microsystems 81(2021) 103719.

[5] F. Chu, R. Zhang, R. Ni, W. Dai, An Improved Identity Authentication Scheme for Internet of Things in Heterogeneous Networking Environments, IEEE 16th International Conference on Network-Based Information Systems, 2013.

[6] S. Echeverría, D. Klinedinst, K. Williams, G.A. Lewis, Establishing trusted identities in disconnected edge environments, 2016 IEEE/ACM Symposium on Edge Computing (SEC), 2016.

[7] A.C. Donald, L. Arockiam, A secure authentication scheme for MobiCloud, IEEE 2015 International Conference on Computer Communication and Informatics (ICCCI), 2015.

[8] J.L. Tsai, N.W. Lo, A privacy-aware authentication scheme for distributed mobile cloud computing services, IEEE systems journal 9(3)(2015) 805-815.

[9] K. Wu, R. Cheng, W. Cui, W. Li, A lightweight SM2-based security authentication scheme for smart grids, Alexandria Engineering Journal 60(1)(2021) 435-446.

[10] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, K.K.R. Choo, Cloud based data sharing with fine-grained proxy re-encryption, Pervasive & Mobile Computing 28(2016) 122-134.

[11] J. Shao, R. Lu, X. Lin, K. Liang, Secure bidirectional proxy re-encryption for cryptographic cloud storage, Pervasive & Mobile Computing 28(2016) 113-121.

[12] A.N. Khan, M.L.M. Kiah, M. Ali, S. Shamshirband, A.U. Khan, A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach, Journal of Grid Computing 13(4)(2015) 651-675.

[13] C.-M. Wu, R.-S. Chang, H.-Y. Chan, A green energy-efficient scheduling algorithm using the dvfs technique for cloud datacenters, Future Generation Computer Systems 37(2014) 141-147.

[14] W. Zhang, Z. Zhang, H.-C. Chao, F.-H. Tseng, Kernel mixture model for probability density estimation in bayesian classifiers, Data Mining and Knowledge Discovery 32(3)(2018) 675-707.

[15] M. Portnoy, Virtualization essentials, John Wiley & Sons, 2012.

[16] Q. Peng, A. Walid, J. Hwang, S.H. Low, Multipath tcp: Analysis, design, and implementation, IEEE/ACM Transactions on Networking (ToN) 24(1)(2016) 596-609.

[17] P. Liu, D. Willis, S. Banerjee, ParaDrop: Enabling Lightweight Multi-tenancy at the Network's Extreme Edge, IEEE/ACM Symposium on Edge Computing (SEC), 2016.

[18] W. Felter, A. Ferreira, R. Rajamony, J. Rubio, An Updated Performance Comparison of Virtual Machines and Linux Containers, 2015 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), 2015.

[19] B.S. Hu, Q. Liu, X.H. Liu, T. Peng, G.J. Wang, J. Wu, DABKS: dynamic attribute-based keyword search in cloud computing, 2017 IEEE International Conference on Communications (ICC'17), 2017.