Research on Identity Authentication Framework Model Based on Cloud Computing

Nan Hu, Zhenjiang Lei, Lei Wang and Yubo Liu

State Grid Liaoning Elect Power Supply Co Ltd, Informat & Commun Co, Shenyang, Liaoning, China

879527755@qq.com

Keywords: Cloud computing; Neural network model; Identity authentication framework

Abstract: Identity authentication scheme that combines security, recognition rate, and operational efficiency in cloud computing environment is proposed in this paper, which utilizes fully homomorphic encryption on integer ring optimized to protect identity feature information security, and neural network model is used to identity feature extraction. Moreover, by converting Euclidean distance calculation among identity feature vectors into dot product calculation during identity recognition, computational complexity is reduced. Finally, based on Store Front authentication architecture of Citrix desktop cloud system, identity-based desktop cloud authentication system is designed, and identity authentication scheme is implemented through API interface provided by Citrix Store Front component. What's more, experimental verification is performed in actual distributed environment so that security and feasibility of solution can be analyzed, which shows that this solution can not only improve security of identity authentication, but also have high recognition rate and operating performance to meet requirements of practical applications.

1 Introduction

Nowadays, under cloud computing environment, identity authentication schemes are mainly divided into two categories. One is to perform multi-factor identity authentication scheme with the help of shared memory information such as identity and passwords, calculated storage information such as smart cards and mobile devices, as well as unique biometric information. The other is cryptography-based authentication scheme that uses public key cryptography technology and digital certificate including signature to authenticate identity of participants. Moreover, identity authentication scheme in cloud computing environment does not depart from traditional identity authentication model and framework, which not only has security problems in traditional identity authentication methods, but also has new problems such as insufficient privacy protection and poor practicality [1].

Compared with other biometric recognition technologies, identity recognition is a more intuitive and effective identity authentication method, where not only equipment cost is lower, but authentication method is more friendly. Moreover, identity-based identity authentication first collects identity characteristics of users which are stored in database as template. When user logs in, identity characteristics collected on-site are compared with identity characteristic templates in database. Then, based on similarity of the two, identification is performed to verify user identity legitimacy, the key to security of which lies in security of identity feature template [2]. Besides it, homomorphic encryption technology can solve problem of two existing identity feature template protection schemes feature transformation and biometric encryption, which cannot achieve high security identity authentication in complex network environments. However, after adding password protection policy, compared with existing identity recognition system, it will have certain impact on identity recognition rate due to additional calculation and communication overhead [3].

2 Architecture of Identity-based Authentication System in Cloud Computing Environment

Relying on Citrix desktop cloud virtualization solution, identity-based desktop cloud identity

DOI: 10.25236/icme.2019.064

authentication system adopts client / server model, whose architecture is shown in Figure 1 where client is all-in-one cloud terminal with embedded HD camera, and server is composed of Centos-based authentication server cluster and Citrix's Store-Front authentication component.

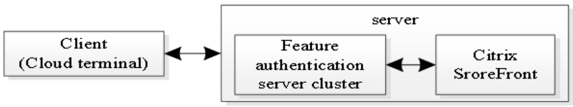

Fig.1 System Architecture and Identity Authentication Process

This section gives specific algorithms and processes of FHE-based identification in cloud computing environment, and describes key methods and technologies involved in solution in detail[4-5].

After cloud terminal namely client completes identity detection, preprocessing and feature extraction, it sends identification request to authentication server and waits for response from authentication server. Once authentication server receives identification request from cloud terminal, it responds immediately and feeds back processing result of classification recognition to cloud terminal. Process is shown in Figure 2.

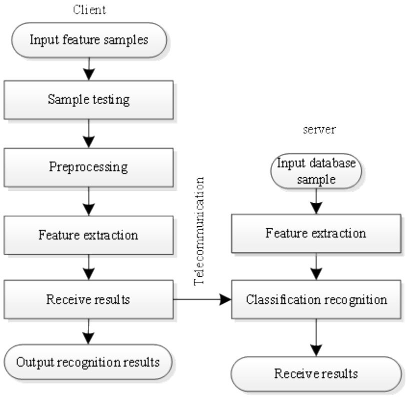

Figure 2 Architecture of Identity System in Cloud Computing Environment

Assuming client has vector x=(x_1,x_2,……,x_n), and server has vector y=(y_1,y_2,……,y_n), if $x' = (x1, x2, \ldots\ldots, xn, \sum_{i=1}^{n} x^2{}_i)$ and $y' = (-2y_1, -2y_2, \ldots\ldots, -2y_n, 1)$, Euclidean distance of *x* and *y* can be obtained through *x '* and *y'*.

$$d(x,y) = \sum_{i=1}^{n}(x_i - y_i)^2 = \sum_{i=1}^{n}(x_i)^2 + \sum_{i=1}^{n}(y_i)^2 - 2\sum_{i=1}^{n} x_i y_i = x' ? y' + \sum_{i=1}^{n} y_i^2 \qquad (1)$$

Since server has already owned $\sum_{i=1}^{n} y_i^2$, two parties only need to exchange one round information, and Euclidean distance *d (x, y)* of two identity feature vectors can be obtained through calculating x '· y'. Flow of operation phase is shown in Figure 3[6-7].

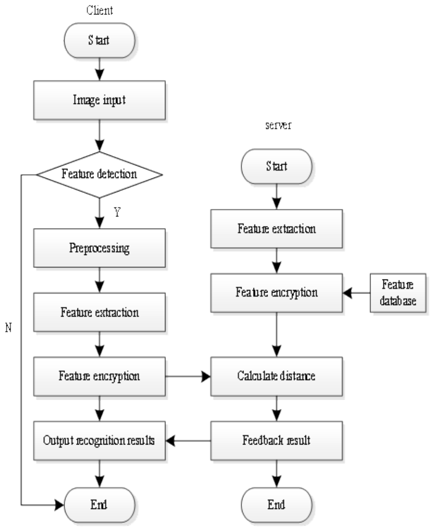

Fig.3 Authentication Phase Process

(1)When user logs in, cloud terminal uses identity image captured by camera to perform corresponding operations so that identity feature vector *x* can be obtained. Then, *pk* is adopted to encrypt $x'(x'=(x_1,x_2,\ldots\ldots,x_n,\sum_{i=1}^{n} x_i^2))$ and send obtained ciphertext Enc (x ') to authentication server.

(2)Authentication server will extract feature vector matrix of all identities to obtain *m* feature vectors where *m* is the number of feature vectors in identity database data. Then, *pk* is used to encrypt $y'(y'=(-2y_1,-2y_2,\ldots\ldots,-2y_n,1))$ for each feature vector to get Enc (y '). Moreover, dot product of Enc (x ') and Enc (y') is calculated and $\sum_{i=1}^{n} y_i^2$ is accumulated. Besides it, *sk* decryption is used to calculate Euclidean distance of *m* pairs of feature vectors, where the minimum distance is the result of identity classification recognition [8].

3 Efficiency and Safety Analysis

In order to test effectiveness of solution, separate authentication server is added to Citrix desktop cloud solution, and implemented authentication module based on Python and Dlib in authentication server. In addition, performance of server used in experiment is IntelXeonE5-2650v4, main frequency is 2.2GHz, and memory is 32GB. Besides it, five computing nodes, 1 management node and 1 service node are deployed in authentication server. What’s more, identity characteristics database is derived from LFW identity database and a total of 500 identities from 10 persons to be tested. Functional tests are arranged in the environment of single feature information and multiple feature information, and test results are as follows.

Tab.1 Accuracy Test

	Single feature information	Multi-feature information	
1: N certification		clear	blurry
	99.5	99.1	95

In complex feature information environment, identity recognition rate of this solution can reach more than 99%, and in 1: N authentication mode, it can meet needs of practical applications. However, in multi-feature information fuzzy environment, since captured identity information is weak, where unclear details and lower accuracy occur, identity recognition rate has decreased. Therefore, under normal office conditions, system can meet functional needs of users.

Theoretical expectation of identity concurrency identification in this scheme is 30 concurrent per second. What's more, identification request to authentication server under normal office scenarios is simulated through writing client-side script, and the maximum number of requests allowed by system is checked through continuous system load. What's more, it can be seen from Table 2 that when the number of simulated concurrent identification requests exceeds 30 and reaches 50, which obviously exceeds load authority of authentication server, abnormal situation occurs in which the request does not respond, which shows that this solution can meet 30 concurrent requests per second in configured test environment.

Tab.2 Performance Test under Different Loads

Number of simulated users	Average delay / ms	Received response rate /%	Response accuracy rate /%
10	25	100	99.7
30	30	100	99.5
50	2655	34	100

Security analysis of this solution is analyzed from server, client, and network security.

(1)Server security analysis: All identity feature templates stored in server are encrypted. Even if attacker obtains permissions of database through illegal channels, it is almost impossible to crack data stored in database after FHE public key encryption through brute force without private key. Therefore, this solution can effectively protect identity signature template from internal attacks originated from authorized servers.

(2)Client Security Analysis: During identification, even if hacker is lurking in client, only encrypted data can be obtained, and no identity information of any user can be obtained. Meanwhile, since client is cloud terminal based on closed Linux system, users cannot perform any operations on cloud terminal system.

(3)Network Security Analysis: Even if attacker has listened to communication between client and server, which is able to steal interaction data between client and server, identity characteristic data transmitted among them has been encrypted by full homomorphic encryption scheme. Attacker only obtains a bunch of ciphertexts, and plaintext information cannot be recovered. Therefore, solution proposed in this paper can prevent insecure network sniffing and intermediate data attacks.

4 Conclusion

Identity authentication scheme that integrates FHE and identity under cloud environment is proposed in this paper to ensure security of key generation, distribution, and identity authentication. However, in complex cloud computing environment, in order to greatly ensure user data and privacy, it is also necessary to analyze security issues of actual cloud platform.

This paper is funded by "Research on Key Technologies of Trusted Identity Authentication for Core Business of Power Grid (Project Number: 5222XT180030)".

References

[1] Zhang Fan. Construction of Fine-grained Theme Emotion Hybrid Model in E-commerce Review [J]. Business Economics Research. 2017 (24)

[2] Song Fengyi, Hu Tai, Yang Ming. Fine-grained recognition of composite attribute learning based on appearance [J]. Data Acquisition and Processing. 2016 (06)

[3] Chen Ziyan, Huang Yu, Wang Yang, et al. A method for improving fine-grained sentiment analysis using semantic similarity features [J]. Computer Applications and Software. 2017 (03)

[4] Zhang Jie, Dong Hui. Research on fine-grained trusted management framework in pervasive environment [J]. Measurement and Control Technology. 2017 (05)

[5] Zhu Yangguang, Liu Ruimin, Wang Zhen, et al. Fine-grained image recognition based on joint

optimization multi-task learning [J]. Journal of Shaanxi University of Technology (Natural Science Edition). 2019 (06)

[6] Tang Xiaobo, Liu Guangchao. A Review of Fine-Grained Sentiment Analysis Research [J]. Library and Information Work. 2017 (05)

[7] Hongwen Hui, Chengcheng Zhou, Shenggang Xu, Fuhong Lin, A Novel Secure Data Transmission Scheme in Industrial Internet of Things, China Communications, vol. 17, no. 1, pp. 73-88, 2020.

[8] Fuhong Lin, Yutong Zhou, Xingshuo An, Ilsun You, Kim-Kwang Raymond Choo, Fair Resource Allocation in an Intrusion-Detection System for Edge Computing: Ensuring the Security of Internet of Things Devices, in IEEE Consumer Electronics Magazine, vol. 7, no. 6, pp. 45-50, 2018. doi: 10.1109/MCE.2018.2851723.