A High Security Distance Education Platform Infrastructure Based on Private Cloud

https://doi.org/10.3991/ijet.v13i10.9450

Jingtai Ran, Kepeng Hou(✉), Kegang Li
Kunming University of Science and Technology, Yunnan, Kunming, China.
2764403681@qq.com

Niya Dai
Yunnan Metropolitan Construction Investment Group Co., Ltd, Yunnan, Kunming, China.

Abstract—This paper aims to avoid the tampering or leakage of sensitive data in a distance education platform. To this end, an intelligent identity authentication model was proposed to realize continuous user authentication, and high security infrastructure was designed for distance education platform based on the proposed model. The experimental evaluation shows that the proposed infrastructure based on private cloud can greatly improve the security of distance education platform. Suffice it to say that the research findings provide new insights into the security of distance education.

Keywords—Distance education, Information security; Private cloud; Public key infrastructure (PKI); Cloud computing

1 Introduction

Distance education refers to the education of students not physically present in a classroom [1-2]. The delivery of distance education has been greatly facilitated by the proliferation of computers and the Internet. Now, virtual reality technology has enabled many schools to provide all their curricula online [3].

The benefits of distance education include extending education opportunities to general populace and businesses, expanding the communication channels in education, and enabling disabled or sick students to receive education at home. Nevertheless, the effect of distance education is still restricted by issues like information security.

The openness of distance education systems both brings about high accessibility and numerous anomalous logons, adding to the difficulty in user identification. In this case, the course teaching will be slowed down and the education effect will be impacted. Hence, user authentication has become a hot topic in the research on distance education. Some biometrics technologies like fingerprint identification have been proposed for user authentication, but they have been proved privacy-intrusive [4]. Based on the Internet of Things (IoT), hardware authentication methods can guarantee the security of distance education systems. However, the same protocol applies to the communication between all systems, making it easy to impersonate the users.

In this paper, a user authentication model was developed for distance education platform based on private cloud, aiming to avoid the tampering or leakage of sensitive data. The model was created with the public key infrastructure (PKI) security mechanism [5] and private cloud technology [6]. Following our model, the high-security infrastructure can verify student identities for the safety of the entire system.

The rest of this paper is organized as follows: Section 2 reviews the existing literature on distance education; Section 3 presents the distance education platform based on private cloud; Section 4 creates the distance education intelligent identity model; Section 5 introduces the continuous user authentication method based on face recognition and biometric traits; Section 6 applies the proposed model in experiments and analyses the experimental results; Section 7 wraps up this research with some meaningful conclusions.

2 Literature review

The security vulnerabilities [7] of distance education system give attackers the chance to hack into the system. Miguel et al. suggested that the traditional security methods cannot fulfil the security requirements of distance education platform [8]. Yee et al. argued that distance education platform must be adequately protected from unauthorized use [9]. So far, some PKI solutions [10-11] have been developed to provide a reliable guarantee to distance education platform.

Many scholars agree that it is necessary to verify student identities for distance education platform. For this purpose, education data mining [12] was proposed as an innovative way for identity verification. Since its birth, education data mining has been the focal point of education research. For instance, Caballe et al. put forward a novel method to extract useful knowledge from the data generated from distance education platform [13], laying the basis for some innovative user authentication strategies. Santi et al. developed a method to verify the actual student identities in distance education [14].

The cloud computing, an immensely popular technology, has been introduced to enhance the security of distance education platform. Based on cloud computing, Dong et al. fabricated physical machines to realize security on-demand for distance education platform [15]. Cayirci et al. designed a highly private and secure military cloud system which ensures the security at multiple levels [16].

To sum up, the existing security mechanisms mainly rely on a single measure (e.g. two-step verification) to ensure the safety of distance education platform. Nonetheless, the identity verification in distance education platform should not stop at the login process, but go on as long as the student is connected to the platform. Therefore, the author designed highly-secure infrastructure for distance education platform, capable of verification through the user’s active period on the platform.

3 Distance education platform based on private cloud architecture

The main objective of the private cloud is to establish on-demand infrastructure for distance education applications, seeking to relieve the increasing pressure on distance education programs and modules. Figure 1 illustrates the hardware of the private cloud architecture.

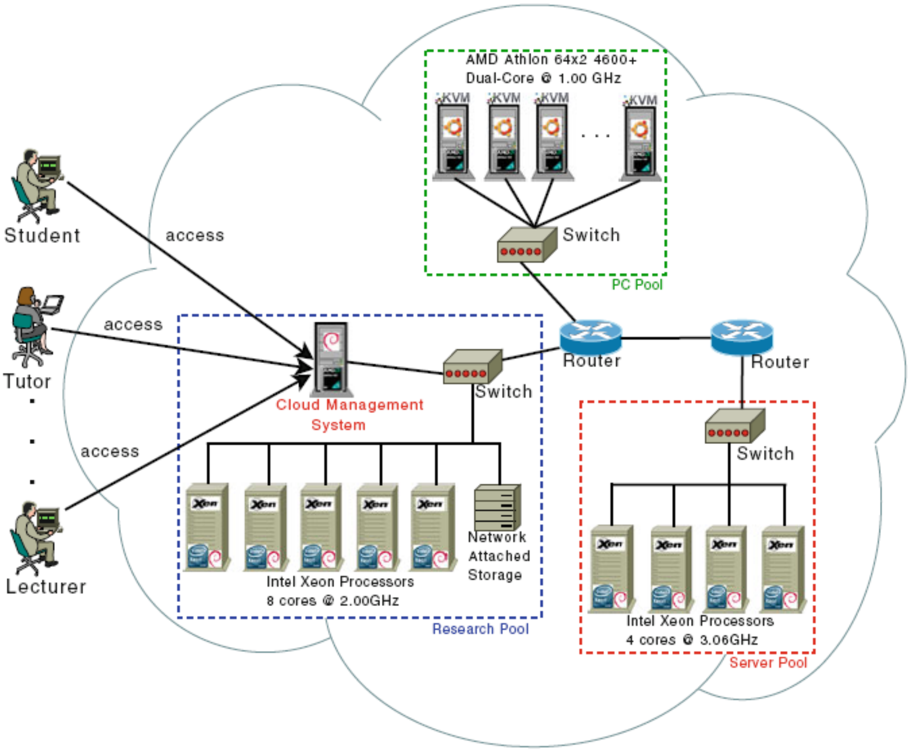

Fig. 1. Private cloud architecture

The architecture consists of three computer pools, each of which is managed by the cloud management system (Figure 2).

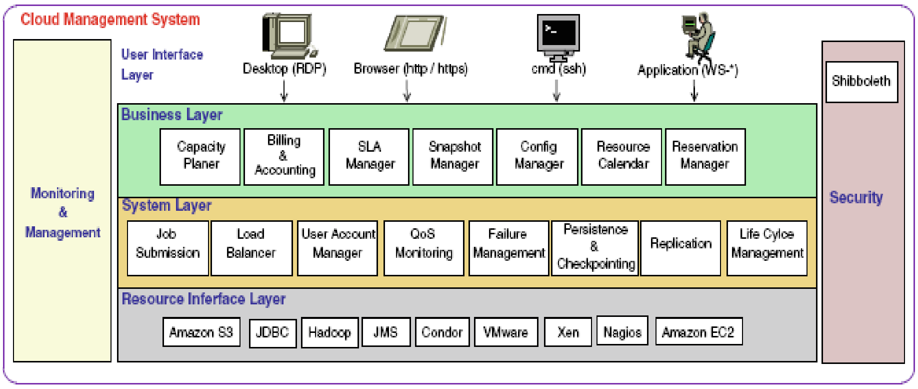

Fig. 2. Cloud management system

The cloud management system was divided into several layers, which work together to ensure the security of services and user data. The user interface layer provides different access points to the cloud system; the business layer regulates resource supply and demand; the system layer monitors the daily operation; the resource interface layer deals with the hardware.

This section only focuses on the security components designed to meet the student needs. Among them, Shibboleth is a component based on the single sign-on solution. It is responsible for authenticating the access to the cloud platform and distance education services. Figure 3 displays the flowchart of Shibboleth-based authentication.

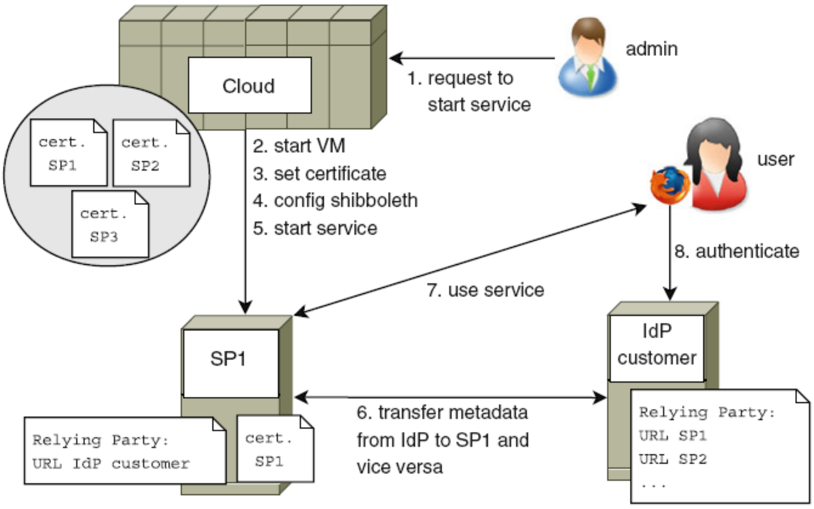

Fig. 3. Shibboleth-based single sign-on solution for cloud computing

The following steps must be covered for a student to use the web service: (1) the admin requests to start a web service on the cloud platform; (2) a virtual machine installed with the web service is started; (3) the relevant certificate is copied to the virtual machine; (4) the Shibboleth is configured; (5) the web service is started; (6) Shibboleth exchanges the meta data; (7) it is the first time for the student to call them service; (8) the student identity is authenticated.

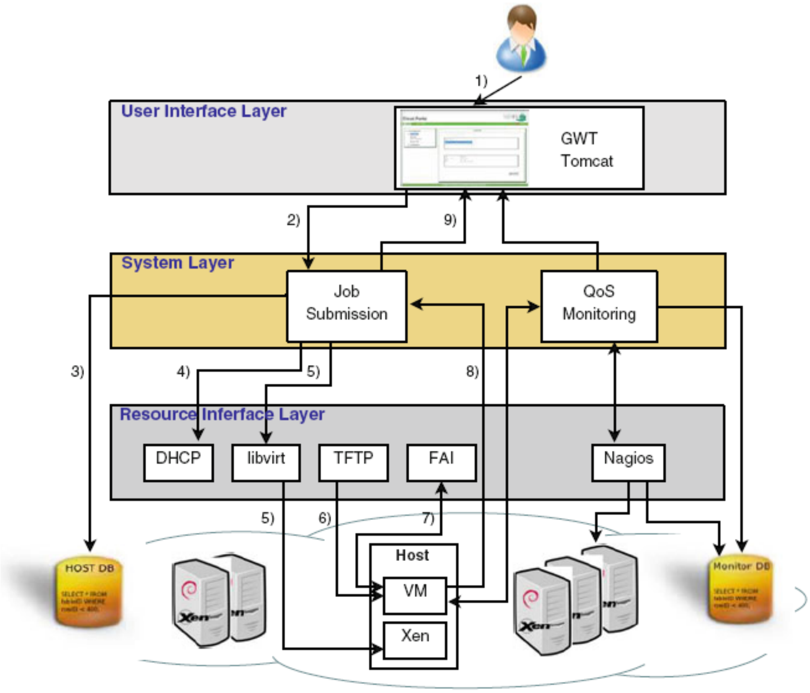

Fig. 4. Automatic creation of virtual machine

Hereinto, the key step lies in the automatic creation of the virtual machine. The components involved in this step are presented in Figure 4.

Once started, the virtual machine can be reserved by the student. To access the virtual machine, the student has to log in the web portal (Figure 5). After authentication, he/she will be able to use resources deployed on the cloud platform.

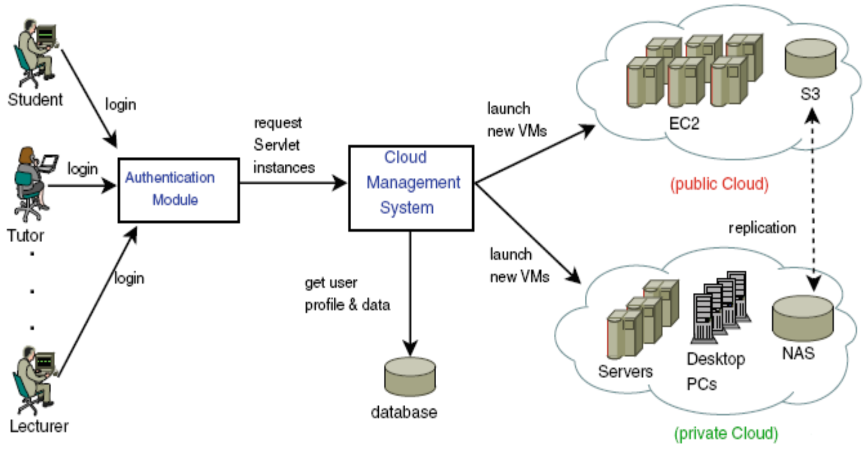

Fig. 5. The process of accessing the resources deployed on the cloud platform

4 Distance education intelligent identity model

This section introduces the student authentication model for distance education platform based on a multi-fold security approach. In the distance education platform, it is essential to verify student identities during course teaching and assessment activities. To this end, a PKI-based security module was designed and named as intelligent identity agent. The module integrates many authentication methods for distance education platform. Figure 6 gives an example of our model.

In the example, the authentication levels of a new course can be created by the authentication level designer module, and the most suitable authentication methods can be selected from the authentication methods repository. For instance, the designer may select the two-step verification and biometrics. The former refers to login with password and SMS verification (login+SMS), while the latter stands for biometric methods like fingerprint identification.

The authentication methods repository contains both classical methods and biological/behavioural validation methods, namely, email verification (user-password), two-step verification (login + SMS), tuning test (Captcha), face recognition, fingerprint identification, speech recognition and keystroke recognition [17].

In the above method, face recognition is the most popular one, and can be used in conjunction with speech recognition. The combined recognition method goes as follows. First, the user profile must be created in advance by the camera and the microphone. Facing the camera, the user should read the alphabet letter by letter to the microphone. Then, the system will find the pattern of the phonetic alphabet with artificial intelligence algorithm, and set up an ID record for the user. When a person authenticates himself/herself to the system, the sound intensity and body features (e.g. face and mouth gestures) will be compared to the ID record. The whole process is illustrated in Figure 7.

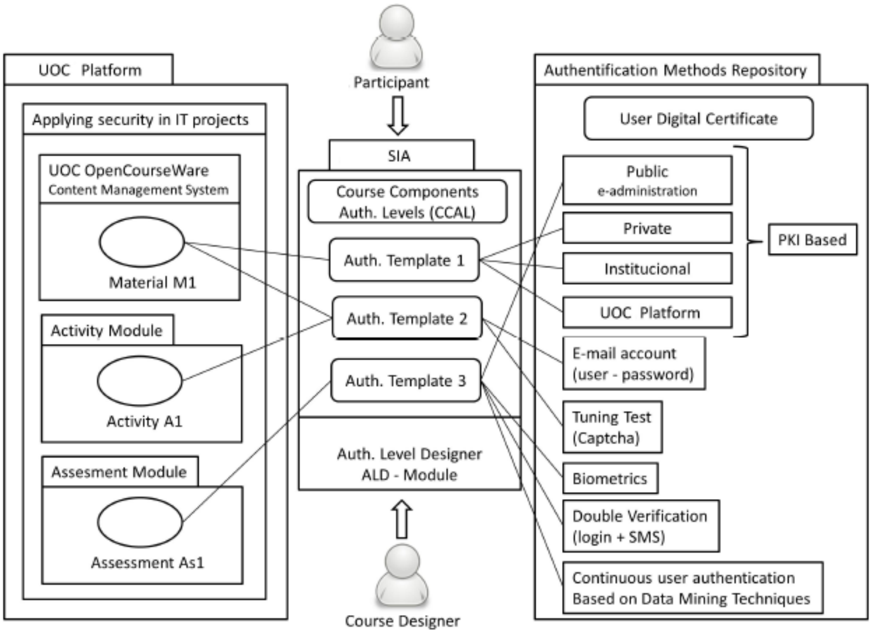

Fig. 6. Intelligent identity model

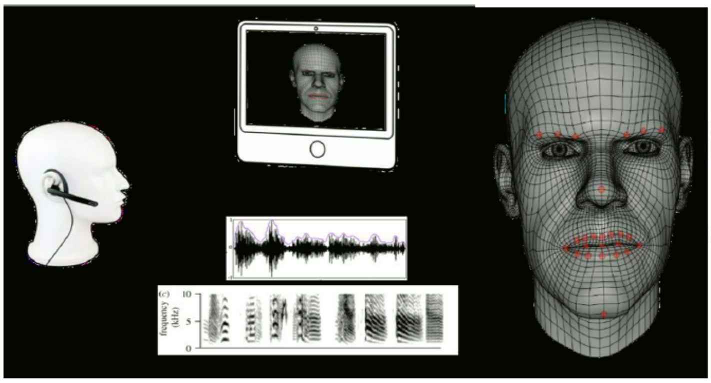

Fig. 7. The critical technologies of the face recognition-speech recognition coupling method

5 Continuous user authentication method based on face recognition and biometric traits

This section presents the continuous authentication method that continuously monitors and authenticates the user as long as he/she is connected to the distance education platform. The block diagram of the method is given in Figure 8.

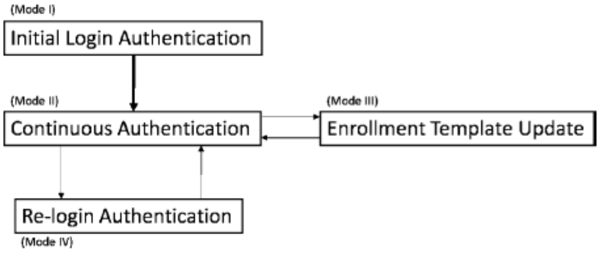
(Mode I)
Initial Login Authentication
(Mode II)
Continuous Authentication
(Mode III)
Enrollment Template Update
Re-login Authentication
(Mode IV)

Fig. 8. The framework of the continuous user authentication method

As shown in Figure 8, the initial login authentication (Model I) contains the following steps: 1) password authentication; 2) face detection; 3) localization of body with face; 4) template enrolment. The continuous authentication (Mode II) starts right after Mode I. This mode authenticates the user by the enrolment templates in Model I through 1) face and body identification; 2) face recognition; 3) similarity computation. If the similarity falls below the given threshold, enrolment template update (Mode III) should be initiated. Mode III has two steps: 1) illumination change detection, 2) updating enrolment templates. For re-login authentication (Model IV), the first three steps are the same as steps 2)~4) in Mode III, and step 4) is the re-authentication of the user using both soft and hard biometrics. The flowchart of the continuous user authentication is shown in Figure 9.

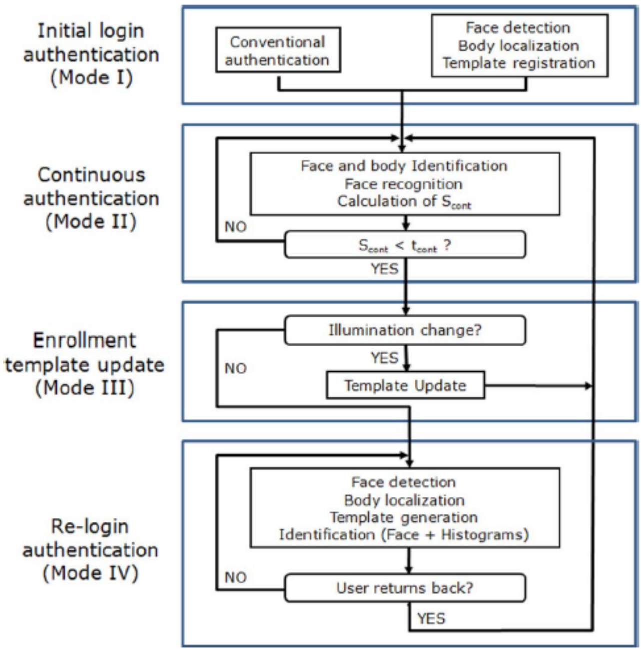
Initial login authentication (Mode I)
Conventional authentication
Face detection
Body localization
Template registration
Continuous authentication (Mode II)
Face and body Identification
Face recognition
Calculation of S_{cont}
NO
$S_{cont} < t_{cont}$?
YES
Enrollment template update (Mode III)
Illumination change?
YES
NO
Template Update
Re-login authentication (Mode IV)
Face detection
Body localization
Template generation
Identification (Face + Histograms)
NO
User returns back?
YES

Fig. 9. The flowchart of proposed continuous user authentication

The continuous user authentication method hinges on face recognition and biometric traits technology. The biometric traits [18] are the prominent features that distinguish between any two persons. Although it cannot identify a user, the biometric traits technology can monitor if the user currently using the system is the one who logged in the system.

Let z_t^{sf}, z_t^{hf} and z_t^{c} denote the set of soft-face biometrics, the set of hard-face biometrics, and the set of clothes colours. Then, the similarity for the three kinds of biometric information can be calculated as:

$$S_{softface} = s(z_t^{sf}, z_0^{sf}) \tag{1}$$

$$S_{hardface} = s(z_t^{hf}, z_0^{hf}) \tag{2}$$

$$S_{clothing} = s(z_t^{c}, z_0^{c}) \tag{3}$$

Thus, the total biometric score can be calculated as follows:

$$S_{cont} = \omega S_{softface} + (1 - \omega) S_{clothing} \tag{4}$$

where ω is the weighted value of the combined biometric traits of face and clothes. If $\boldsymbol{S_{cont}}$ is greater than the threshold t_{cont} , the user is proved genuine.

The similarity of the hard face biometrics $\boldsymbol{S_{hardface}}$ only applies to the re-login authentication:

$$S_{re-login} = F(T_{cur} - T_{reject})\boldsymbol{S_{cont}}$$

where $F(\Delta t)$ is the time decay function; T_{cur} is the current time when $\boldsymbol{S_{hardface}}$ exceeds the threshold; T_{reject} is the time when a user is rejected by the continuous authentication.

The following three conditions must be satisfied for re-login authentication:

$$S_{hardface} \geq t_{hardface} \tag{5}$$

$$T_{cur} - T_{reject} \leq t_{delay} \tag{6}$$

$$S_{re-login} \geq t_{re-login} \tag{7}$$

where t_{delay} and $t_{re-login}$ are threshold values.

6 Experiments and analysis

The client of the high security distance education platform (Figure 10) involves a laptop and a webcam.

Fig. 10. The client of the high security distance education platform

Twenty students were invited to use the distance education platform, and several threshold values were employed for the authentication. The relationship between the similarity and student action in front of the webcam is recorded in Figure 11.

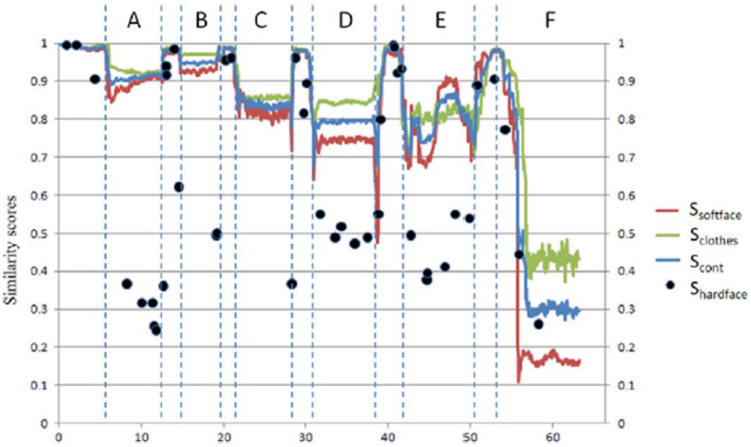

Fig. 11. The variation in similarity

As shown in Figure 11, the similarity score varies from 0 to 1. The higher the score, the better the similarity between the user being authenticated and the user who has logged in the platform. The similarities $\boldsymbol{S_{clothing}}$, $\boldsymbol{S_{softface}}$, and $\boldsymbol{S_{cont}}$ remained high regardless of student posture, but plunged once the student walked away from the client. By contrast, the hard face similarity $\boldsymbol{S_{hardface}}$ was not very stable.

Then, an experiment was conducted to detect illumination changes, and thus verify the robustness of the proposed method. Figure 12 shows the temporal-variation in similarities with or without updating enrolment templates.

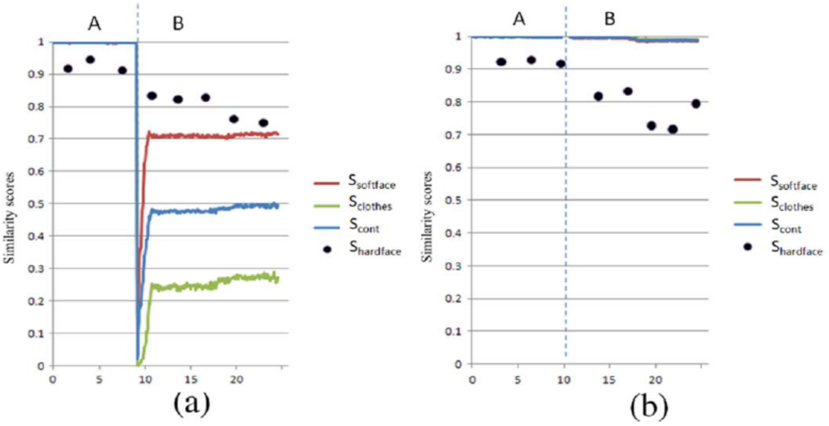

Fig. 12. The similarity score with and without updating enrolment templates (a) Without updating enrolment templates; (b) With updating enrolment templates

In Figure 12(a), the similarity score decreased rapidly once an illumination change was detected. On the contrary, the score remained high despite the illumination change (Figure 12 (b)).

7 Conclusions

The student authentication is one of the greatest barriers to further development of the popular distance education platform. To solve the problem, this paper develops an intelligent identity authentication model based on private cloud. Considering the features of distance education, the model provides an authentication methods repository, which is flexible enough to ensure the safety of course and student. Compared with the existing methods, our method can realize continuous authentication, i.e. denying the access of imposter until the initial user logs out. Although it provides more security than existing methods, the proposed method faces constraints of network bandwidth and computer hardware. In the future, the author will consider introducing two cameras to capture depth information and evaluating the whole platform in routine operating environments.

8 References

[1] Kaplan, A.M., Haenlein, M. (2016). Higher education and the digital revolution: About MOOCs, SPOCs, social media, and the Cookie Monster, Business Horizons, 59(4): 441-450. https://doi.org/10.1016/j.bushor.2016.03.008

[2] Dick, G.N., Hanna, M. (2002). Is On-Line Distance Education a Viable Alternative for Undergraduates. An Experiment with the Students in Georgia, the Professor in Australia, Computer Assisted Instruction, 22(1): 13-19.

[3] Aslan, A., & Zhu, C. (2018). Starting teachers' integration of ICT into their teaching practices in the lower secondary schools in Turkey. Educational Sciences: Theory & Practice, 18(1), 23–45. https://doi.org/10.12738/estp.2018.1.0431

[4] Kravvaris, D., Kermanidis, K.L., Ntanis, G. (2016). How MOOCs Link with Social Media, Journal of the Knowledge Economy, 7(2): 461-487. https://doi.org/10.1007/s13132-014-0219-2

[5] Uruena, M, Machnik, P, Niemiec, M. (2014). Security architecture for law enforcement agencies, Multimedia Tools and Applications, 75(17): 1-24.

[6] Ouf, S., Nasr, M. (2011). An Ecosystem in e-Learning Using Cloud Computing as platform and Web2.0, International Journal of Acm Jordan, 2(1): 134-140.

[7] Wei, W.S., Meng, X.X., Li, H.H. (2011). Digital Signature Technology Research of Distance Education Network Security Authentication, Advanced Materials Research, 267(1): 831- 836. https://doi.org/10.4028/www.scientific.net/AMR.267.831

[8] Miguel, J., Xhafa, F., Prieto, J. (2015). Security in online web learning assessment, World Wide Web-internet & Web Information Systems, 18(6): 1655-1676.

[9] Yee, G., Xu, Y., Korba, L. (2002). Privacy and Security in E-Learning, Future Directions in Distance Learning & Communication Technologies, 1(4): 234-238.

[10] Miguel, J., Caballe, S., Prieto, J. (2012). Providing Security to Computer-Supported Collaborative Learning: An Overview, International Conference on Intelligent NETWORKING and Collaborative Systems, IEEE, 97-104. https://doi.org/10.1109/iNCoS.2012.60

[11] Miguel, J., Caballe, S., Prieto, J. (2013). Information Security in Support for Mobile Collaborative Learning, Seventh International Conference on Complex, Intelligent, and Software Intensive Systems, IEEE, 379-384. https://doi.org/10.1109/CISIS.2013.69

[12] Romero, C., Ventura, S. (2010). Educational Data Mining: A Review of the State of the Art, IEEE Transactions on Systems Man & Cybernetics Part C, 40(6): 601-618. https://doi.org/10.1109/TSMCC.2010.2053532

[13] Caballe, S., Xhafa, F. (2013). Distributed-based massive processing of activity logs for efficient user modeling in a Virtual Campus, Cluster Computing, 16(4): 829-844. https://doi.org/10.1007/s10586-013-0256-9

[14] Santi, C., Thanasis, D., Fatos, X. (2010). Enhancing Knowledge Management in Online Collaborative Learning, International Journal of Software Engineering & Knowledge Engineering, 20(4): 485-497. https://doi.org/10.1142/S0218194010004839

[15] Dong, B., Zheng, Q., Yang, J. (2009). An E-learning ecosystem based on cloud computing infrastructure, Ninth IEEE international conference on advanced learning technologies, ICALT, 125-127.

[16] Cayirci, E., Rong, C., Verkoelen, C. (2009). Snow leopard cloud: a multi-national education training and experimentation cloud and its security challenges, the 1st international conference on cloud computing, 57-68.

[17] Clarke, A.M. (2011). Specifications and characteristics of a soundproofed, electrically shielded and thermally insulated room, Australian Journal of Psychology, 17(2): 124-132. https://doi.org/10.1080/00049536508255534

[18] Yang, L., Yang, G., Yin, Y. (2014). Exploring soft biometric trait with finger vein recognition, Neurocomputing, 135(8): 218-228. https://doi.org/10.1016/j.neucom.2013.12.029

9 Authors

Jingtai Ran, a male graduate, now is Ph.D. and an assistant researcher who was born in January, 1983 in Chongqing. He works in the Faculty of Land Resource Engineering, Kunming University of Science and Technology, Yunnan, Kunming 650 093, China engaging in student education management and his research direction is higher education. He hosted and finished the sub-project of the "Research on the Development of Teachers' Teaching Ability", a key topic of the 13th Five-Year Plan for China's education supervision. He participated in and completed many projects related to higher education development, and the research results have been widely applied.

Kepeng Hou is from the Faculty of Land Resource Engineering, Kunming University of Science and Technology, Yunnan, Kunming 650 093, China.

Kegang Li is from the Faculty of Land Resource Engineering, Kunming University of Science and Technology, Yunnan, Kunming 650 093, China.

Niya Dai is from Yunnan Metropolitan Construction Investment Group Co., Ltd., Yunnan, Kunming 650 228, China.

Article submitted 31 August 2018. Resubmitted 10 September 2018. Final acceptance 24 September 2018. Final version published as submitted by the authors.