Applying the MCMSI for Online Educational Systems Using the Two-Factor Authentication

https://doi.org/10.3991/ijim.v15i13.23227

Shaymaa Taha Ahmed (✉), Qusay Kanaan Kadhim,

Hamid Sadeq Mahdi, Widyan Salman Abd Almahdy

University of Diyala, Buqubah, Iraq

Shaymaa.taha.ahmed@basicedu.uodiyala.edu / mrs.sh.ta.ah@gmail.com

Abstract—This paper researches the evolution process of what is called two-factor authentication technique and its adaptation related to the educational system through the Internet. This technique is a measure of security employed, particularly in scopes which have valuable information like bank services. It witnesses developments so far as today, in parallel with the developments occurring in technology. Since this technique consists of two phases, the security is going to be developed. Today, bank services, devices using the Internet of things, tickets of public transportation and lots of other scopes are utilized. In the information field, the researchers and scientists always update the techniques of two-factor authentication to resist the attacks related to security. Last years, the researchers studied novel technologies like behavioral biometric or biometrics. The training through the Internet may become much more useful than going to someplace to study a specific course. Mostly, the participants in the trainings through the Internet get many certificates for success, participation, etc. The principal problem is how to certify the truthiness of the participant who desires to get the certification. In this paper, and by researching the techniques of two-factor authentication, the Mimic Control Method with Sound Intensity (MCMSI) is proposed to be used for the training through the Internet.

Keywords—Authentication, Two-Factor, Training, Features, Behavioral, Biological, MCMSI

1 Introduction

At present, fast evolutions in the section of information technology are significant to security. As information security is indicated, the most popular method is the technique of two-step authentication. When the user wants to access to any mobile application, web site, or electronic device, etc., then a two-step control is required from the user by asking the another information such as password, biometric information iris, fingerprint, face recognition [1], [2] .Through the years, options of two-factor authentication have been diversified along with evolutions in technology. Till today, three headlines can form the techniques of two-step authentication [3]. Hardware-based encryption and

related techniques are using graphical/alphanumeric encryption, biological and behavioral features [4] .The biological and behavioral properties can be divided into two features as physical biology and behavioral biometry. Behavioral biometrics includes compiling information such as walking information and location traces. In the future, evolutions in technology point to us two-step verification will require additional behavioral biometric properties. First areas that witnessed the developing of two-step verification were finance and banking where security is very significant. At present, lots of areas like NFC devices, smart home, public transport tickets, transportation use two-step verification [5] . Information spreading to these areas illustrates the significance of evolutions in technology and information immorality increasing and information verification [2]. In modern life, the management of time is necessary. Therefore, many people are participating in training through the Internet to enhance themselves. These training permits the person to participate in currencies anywhere in the world and receive certificates [6]. In this manner, considerable time will be saved in terms of time and material [7]. Many people can misuse education through the Internet. Without authentication, the truthiness of student cannot be known by the provider of education. In this system, a measure like a two-step verification is used to provide the desired security [8]. The entire slot of time that is used by the student to connect to the system should have identity verification, as well as the login screen, to determine the authenticity of the person. Therefore, verification for the entire active period in the system should be necessarily performed. This verification can be done by using numerous enhancements on the method of two-step verification, which is when the user enters any site [9] . This research provides examining up to date techniques of the two-factor authentication and searching and adapting the most suitable technique of verification for education through the Internet.

2 Methods of Authentication

Requesting multiple information from a user to log in a specific system creates a security structure called the two-step authentication. This is similar to possess two locks on the outer door to block theft in our own houses. A two-factor authentication confirmation will occur when the thief plays one of the two keys since he will need the other key. This means that performing a two-factor authentication on the door [10]. Nonetheless, the door locks can be broken without a key when the technology is used. Therefore, kind of features can be added to the two-factor authentication and should be enhanced depending on science. As an example of these features are the biometric features like face recognition and fingerprints, which have been added to guarantee the adaptation of the two-stage verification with nowadays conditions [11].

2.1 One-factor authentication

This authentication depends only on one factor like username or password. Most of the users use simple passwords to remember them easily like "12345" or "love" and so on. However, it seems that the passwords which have capital letters, small letters, numbers, etc., are difficult to remember by the users [12].

Today, despite the weakness in this method, it still is used in many web sites. In this case, there is nothing to do but raising the realization of the users and strengthening the security infrastructure of the Internet [13].

2.2 Two-factor authentication

This authentication depends at first on the most primitive method. Then it incorporated behavioral and biological features.

1. **Hardware-based two-factor authentication**: ATM smart cards physically used two-factor authentication. In the first stage, the ATM card is placed by the user, and then the password is entered. In this way, the safety of the two- factor is achieved. Despite the safety of this system for many years, but the two-step verification cannot be considered as a very successful method because the ATM card can be copied or stolen by someone else. In addition to this hardware-based method today, biometric two-step verification has begun, such as ATM devices that recognize fingerprints. In the future, transactions will be performed safely by performing two-step verification with behavioral biometrics, without the need for a magnetic-specific hardware structure such as a debit card [12].

When the internet speed was not high, and the usage of a mobile phone was unfamiliar, the two-step verification was first used. Therefore, a device called "RSA SecurID" was used to generate the password. The "RSA SecurID" device is shown in figure 1. In this device, there is an algorithm which is capable of generating a complex PIN number. If persons carry this device in today's conditions, the algorithm can still be considered secure for extensive keys lengths [13].

Fig. 1. RSA SecurID

In 1999, people heard the concept of the Internet of things (IoT) concept. Various devices can connect and communicate with each other in this system by using a similar communication protocol. On the hardware side and with the evolution of IoT and robotics, security has become greatly important [14].

The significance of network security is revealed by the fact that numerous devices are connected to a single network. The use of two-factor authentication in robotics should be inevitable in order to provide this security [15]. Data can be exchanged at a short distance with a low bandwidth by using NFC technology. Two-factor authentication can be provided by using NFC technology on the hardware side. Figure 2 shows the two-step verification using NFC [16].

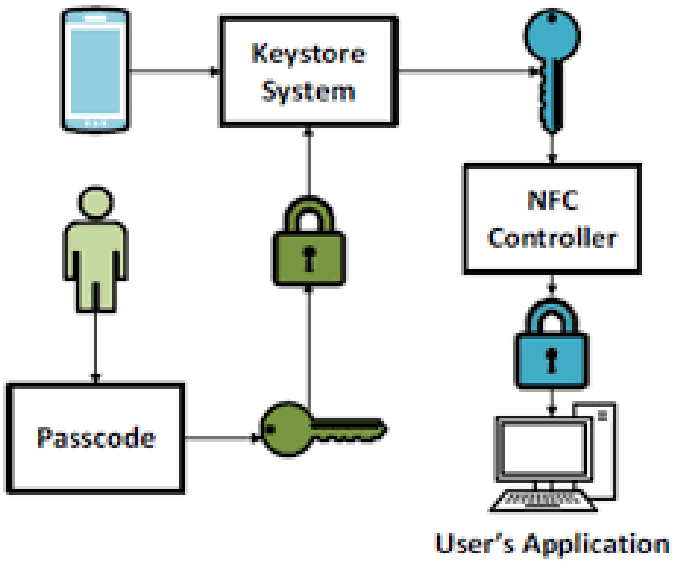

Fig. 2. NFC working principle

NFC has begun to be used especially in cars, at home street gates because the number of NFC-enabled devices has increased. At this point, smaller NFC controllers are used to make users more secure (NFC Controller Chip on mobile phones) [15].

2. **Alpha numerical/ graph-based two-factor authentication:** Today this method can be considered as one of the most usually used two-step verification methods. Its importance appears mainly in the technology of the mobile phone. A general example of its usage can be seen when the password is entered on the input screen of any system by the user. After that, an alphanumeric code coming to the mobile phone enters the corresponding screen to perform the two-factor authentication [16].

Alpha-numeric two-factor authentication suffers from two fundamental problems. The first problem occurs as a result of dependency on the mobile phone by the user who will be unable to access his account, so he cannot perform two-factor authentication in cases like phone corruption. The second problem occurs when the mobile phone is provided with SMS by hackers with various malicious software to forward the code to another phone [14].

The developments in the technologies of touch screen aim graphics-based verification to enter people's lives. A pattern is specified by the user, such as touching a particular point on a pattern or a photo, and the generated graphical password is recorded in the device. Now, the password of the user is this graphical pattern [5].

The graph-based verification suffers from an essential problem is that malicious people can easily observe graphs manually drawn on the screen in public. Android 7.0 version introduced an option to prevent the graphic template drawn from being displayed on the screen. However, this option is still not a suitable measure, since the

graph-based password can be predicted by malicious people from the fingerprints on the screen [17].

The researchers have developed a new technology with enhancements in security like the ability of others to view graphical passwords, predictions from fingerprint traces, and enhancements in the technologies of touch screen and sensor. This technology is called TouchIn. This technology utilizes the 3D accelerometer sensor [3] Direction: x-coordinate, y-coordinate, Speed: x-speed, y-speed, Acceleration: x-acceleration, y-acceleration, Finger press and Hand geometry.

3. **Biological based two-factor authentication:** This authentication in itself is divided into two types, Physiological Biometry and Behavioral Biometry. In physiological biometry, media in the devices are used with the evolution of sensors like fingerprint detection. Behavioural.

Biometry is still a developing technology. Security is provided by evaluating features like thoughts, the brain wave, and person movements [12].

4. **Physiological biometry based on two-step authentication**: In this type, the identity of a person is verified depending on the physical characteristics. The properties used today the fingerprint, iris pattern, retina pattern, face features and hand geometry[18].

In recent mobile phones, many features are used at the same time to provide verification in many ways; these features are like iris recognition, fingerprints, face recognition. In the computer world, face recognition has also been made obtainable to the end-user.

Fingerprinting suffers from one main problem, which is that the system can be entered by malicious people when their finger is torn off, and the relevant sensor is read. The only possible way to prevent this is to read the information of the finger vein instead of fingerprint [17].

5. **Behavioural biometry-based two-step authentication:** This is a method of security verification which can be made by adding the technology evolutions together with the parameters that measure the person's behaviour on the physiological biometrics. Features used by behavioural biometrics remain personal behavior, Location tracks, Brain waves and Thoughts [16].

RhyAuth system with rhythm-based verification has been introduced. This system depends on the creation of a melody with numerous notes. According to the graphical encryption used on the phone, this system is secure, since a melody is created using a long note. Also, this system is suitable for apparent weakness to use two-factor authentication. However, problems can be caused by this system in noisy environments like libraries [19].

In the technology of smart card, password verification has been studied. Using the cryptography method, time-saving is achieved by using the SHA-256 algorithm to validate while waiting for the devices in the queue. This method of authentication has not been fully evolved. However, with future technology evolutions, it will be something that its advantage can be taken by end-users [20].

3 Online Education System

With the development of technology, online training can be taken with the assist of virtual classes (MOOC, etc.) with no limitation in space and time. When a provider gives the training online, the truthness of the person who uses the system is unknown. Therefore, various authentication methods are proposed for online education [21]. These methods contain many verification methods.

3.1 MOOC intelligent identity tool (MOOC-SIA) model

The security method is differentiated by this model as the evaluation part progresses, like activity, homework. etc. Classical lessons use email and password. In more critical areas such as homework, lesson activities, security is expanded further and biometric verification, login and SMS verification, system planning and data mining techniques etc. are based on the information and training of users on the system. Continuous user authentication is provided [22]. The schematic of the MOOC model is shown in Figure 3.

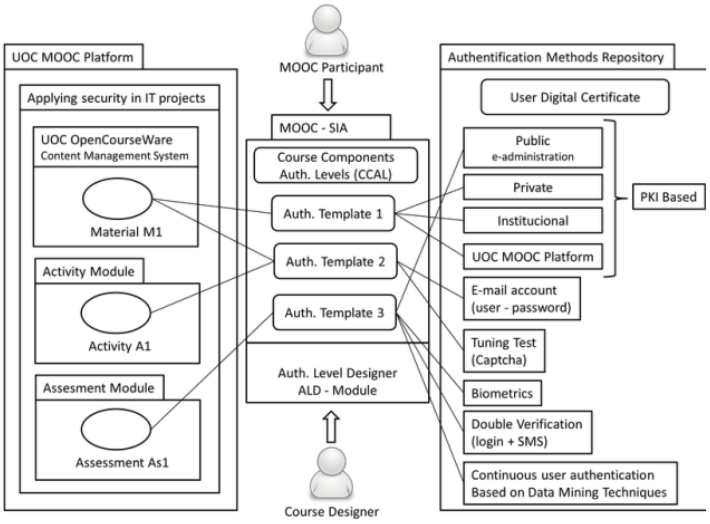

Fig. 3. MOOC intelligent identity tool (MOOC-SIA) model

3.2 Resistance against imitation

The algorithm maintains the security of the system using the following features by deciding whether or not the person has real identity [23]Word Length Frequency, Sentence Length Frequency, Part of Speech Tag Disclosure and Word Specific Frequency.

3.3 Classical methods

Traditional methods are like Fingerprint, Face, Sound as well as Password, SMS, Keystroke. At the same time, biological and behavioural validation are used on the same system. In this method, face recognition is performed by looking at eyebrow, cheek, eye and lip measurements. Volume control is calculated in vector form. In these popular methods we have mentioned above, one of our focus points is constant identity verification based on data mining techniques. Because the system cannot be sure if the user has forged his identity at first. When continuous authentication is done, it is difficult to deceive the system [24].

Even if the operation of this system is correct and does not fail, the system will accept it forever as the right person if the user does not give the correct identity information since the first time it entered the system. It is needed to ensure that the person entering the system is the same person from the first moment to be authenticated in online training. It is important that both the identity information declared at the beginning and at the end of the last one to be compared [25].

3.4 Mimic Control Method with Sound Intensity (MCMSI)

The preparation stage of the MCMSI method [26], [27]

1. The person to be authenticated is created in the system in the real environment.
2. The camera and microphone are used when creating the ID recording on the system.
3. The person who is to be authenticated goes to the camera and reads the alphabet one by one in the microphone. He then reads the primary two- and three-letter hypotheses.
4. With the help of artificial intelligence, the next system finds the phonetic pattern of the phonetic alphabet, which is formed by the syllabic combination of the letters in the alphabet and prompts the user to read the words with this different phonetic pattern.
5. An ID record is created in the system.
6. The working principle of the MCMSI method:
7. Since the face of the system user models the behaviour of Gabor wavelet transform, sensory regions in the human visual system, the feature vector is created, and face recognition control is performed by the facial features.
8. The user reads the words on the screen, and the system controls the user's face and face from the PCA base. On the other hand, the voice of the user controls the voice of the user using the Shell Frequency Cepstrum, Coefficients, Wavelet or Peak frequencies properties.
9. The system overlaps the sound intensity and sound characteristics of the user with the face and mouth gestures, and if these two features are correct, the identity is authenticated.

4 Conclusion

In this investigation, it is conceivable to look at the two-factor authentication techniques, which are state-of-the-art and adjust to the online instruction segment. In the examination, it is seen that two-advance confirmation affirms that individuals are pushing toward conduct biometrics, for example, thinking and perusing.

Education through the Internet is turning out to be increasingly more well-known step by step. Nonetheless, the fundamental issue is that the security verification phase can't be completely accomplished. A unique feature of the person is suggested to be utilized to get this security since it is imitated and kept from being utilized by another person.

A unique authentication is guaranteed by permitting synchronous control of the mouth, mimic movement and sound movement of the person, and this guarantee is done by utilizing the sound and camera. Despite the fact that it has a security level much more than existing systems, there are problems to be defeated like giving the needed internet bandwidth and computer hardware power. With technology advancement, the end-user can theoretically change this system into an applicable structure.

5 References

[1] Qureshi, M. I. et al. (2021) 'Digital Technologies in Education 4.0. Does it Enhance the Effectiveness of Learning? A Systematic Literature Review', International Journal of Interactive Mobile Technologies (iJIM), 15(04), p. 31. https://doi.org/10.3991/ijim.v15i04.20291

[2] Al-Kumaim, N. H. et al. (2021) 'Exploring the Impact of Transformation to Fully Online Learning During COVID-19 on Malaysian University Students' Academic Life and Performance', International Journal of Interactive Mobile Technologies (iJIM), 15(05), p. 140. https://doi.org/10.3991/ijim.v15i05.20203

[3] Ristanto, R. H. et al. (2020) 'Digital Flipbook Imunopedia (DFI) A Development in Immune System e-Learning Media', International Journal of Interactive Mobile Technologies, 14(19), pp. 140–162. https://doi.org/10.3991/ijim.v14i19.16795

[4] Ahmed, S. T., Khadhim, B. J. and Kadhim, Q. K. (2021) 'Cloud Services and Cloud Perspectives: A Review', in IOP Conference Series: Materials Science and Engineering, p. 012078. https://doi.org/10.1088/1757-899x/1090/1/012078

[5] Akinsanmi, O. et al. (2015) 'Two-Factor Authentication Based Automobile Keyless Entry System', (8), pp. 102–106. Available at: https://www.ijeas.org/download_data/IJEAS0208037.pdf.

[6] Badr, A. M., Zhang, Y. and Umar, H. G. A. (2019) 'Dual authentication-based encryption with a delegation system to protect medical data in cloud computing', Electronics (Switzerland), 8(2), pp. 1–14. https://doi.org/10.3390/electronics8020171

[7] Coccia, M. and Watts, J. (2020) 'A theory of the evolution of technology: Technological parasitism and the implications for innovation magement', Journal of Engineering and Technology Management - JET-M. Elsevier, 55(January), p. 101552. https://doi.org/10.1016/j.jengtecman.2019.11.003

[8] Derhab, A. et al. (2020) 'Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing', IEEE Access, 8, pp. 28956–28969. https://doi.org/10.1109/access.2020.2971024

[9] Edna Elizabeth, N. and Nivetha, S. (2017) 'Design of a two-factor authentication ticketing system for transit applications', IEEE Region 10 Annual International Conference, Proceedings/TENCON, (November), pp. 2496–2502. https://doi.org/10.1109/tencon.2016.7848483
[10] Kanaan Kadhim, Q., Sadeq Mahdi, H., & Ail, H. (2018). Storage Architecture for Network Security in Cloud Computing. Diyala Journal for Pure Science, 14(1), 1–17. https://doi.org/10.24237/djps.1401.205c
[11] Gan, T. (2018) 'Construction of security system of flipped classroom based on MOOC in teaching quality control', Kuram ve Uygulamada Egitim Bilimleri, 18(6), pp. 2707–2717. https://doi: 10.12738/estp.2018.6.170.
[12] Gualdoni, J. et al. (2017) 'Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication', Procedia Computer Science. Elsevier B.V., 114(December), pp. 93–99. https://doi.org/10.1016/j.procs.2017.09.016
[13] Kadhim, Q. K., Al-nedawe, B. M. and Hameed, E. M. (2021) 'Encryption and Decryption of Images using GGH Algorithm: Proposed', in IOP Conference Series: Materials Science and Engineering, p. 012063. https://doi.org/10.1088/1757-899x/1090/1/012063
[14] Kakkad, V. et al. (2019) 'A comparative study of applications of game theory in cyber security and cloud computing', Procedia Computer Science. Elsevier B.V., 155(2018), pp. 680–685. https://doi.org/10.1016/j.procs.2019.08.097
[15] Li, Q. et al. (2018) 'Research on user identity authentication based on two-way confirmation in data transmission', MATEC Web of Conferences, 173, pp. 0–3. https://doi.org/10.1051/matecconf/201817303019
[16] Ljubic, S. and Arbula, D. (2017) 'Contact-free interaction with mobile devices using magnetic, lighting and infrared sources', International Journal of Interactive Mobile Technologies, 11(4), pp. 66–82. https://doi.org/10.3991/ijim.v11i4.6712
[17] Kadhim, Q. K., Yusof, R., & Mahdi, H. S. (2018). A Review Study on Cloud Computing Issues. 1st International Conference on Big Data and Cloud Computing (ICoBiC) 2017, 1–11. https://doi.org/10.1088/1742-6596/1018/1/011001
[18] Nama, G. F. and Muludi, K. (2018) 'Implementation of two-factor authentication (2FA) to enhance the security of academic information system', Journal of Engineering and Applied Sciences, 13(8), pp. 2209–2220. https://doi: 10.3923/jeasci. 2018.2209.2220.
[19] Ometov, A. et al. (2018) 'Multi-Factor Authentication: A Survey', Cryptography, 2(1), p. 1. https://doi: 10.3390/cryptography2010001.
[20] Ometov, A. et al. (2019) 'Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications', IEEE Network, 33(2), pp. 82–88. https://doi.org/10.1109/mnet.2019.1800240
[21] Orkun, K. and Erol, V. (2017) 'Network Security Issues and Solutions on Vehicular Communication Systems', (June). https:// doi: 10.20944/preprints201706.0001.v1.
[22] Penna, G. Della, Frasca, P. and Intrigila, B. (2019) 'Two factor authentication for e-government services using hardware-like One Time Password generators', Journal of Computer Science, 15(1), pp. 171–189. https://doi.org/10.3844/jcssp.2019. 171.189
[23] Kadhim, Q. K. (2016). Image compression using Discrete Cosine Transform method. International Journal of Computer Science and Mobile Computing, 5(9), 186–192. https://www.researchgate.net/publication/308983925
[24] Rui, Z. and Yan, Z. (2019) 'A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification', IEEE Access. IEEE, 7, pp. 5994–6009. https://doi.org/10.1109/access.2018.2889996
[25] Ruiz, I. L. and Gómez-Nieto, M. Á. (2017) 'Combining of NFC, BLE and Physical Web Technologies for Objects Authentication on IoT Scenarios', Procedia Computer Science. Elsevier B.V., 109, pp. 265–272. https://doi.org/10.1016/j.procs.2017. 05.350

[26] Velásquez, I., Caro, A. and Rodríguez, A. (2018) 'Authentication schemes and methods: A systematic literature review', Information and Software Technology. Elsevier, 94(September 2017), pp. 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

[27] Wang, C., Xu, G. and Li, W. (2018) 'A Secure and Anonymous Two-Factor Authentication Protocol in Multiserver Environment', Security and Communication Networks, 2018. https://doi.org/10.1155/2018/9062675

6 Authors

Shaymaa Taha Ahmed M.Sc. (2015) in (India) Affiliation: University of Diayla Dept.: Computer science/ College: Basic of education Specialization: - Computer science\ information system. Research Interests: Cloud Computing-Deep Learning-Machine learning-AI -Data mining Google Site: Google scholar: https://scholar.google.com/citations?user=GRl_liEAAAAJ&hl orcid.org/0000-0002-4986-2475/ ✉ Shaymaa.taha.ahmed@basicedu.uodiyala.edu.iq & mrs.sh.ta.ah@gmail.com

Dr.Qusay Kanaan Kadhim Affiliation: Bilad Alrafidain University College, Baqubah, Iraq Department of Computer Techniques Engineering ,Middle Technical University, Iraq, Specialization: - +Information Technology and Communication. Research Interests: Cloud Computing, Information security, Cybersecurity, Artificial Intelligence and Data Mining. Google Site: Google scholar: https://scholar.google.com/citations?user=ekBz_JYAAAAJ&hl=en qusaykn@gmail.com & qusaykn@bauc14.edu.iq

Hamid Sadeq Mahdi Alsultani M.Sc. (at 2007) in (Iraq) Affiliation: University of Diyala Dept.: Computer Science/ College: Basic Education. Research Interests: Natural Language Processing, Information Extraction, Information Retrieval, Machine Learning, Deep Learning and Cloud Computing. Google Site: Google scholar: https://scholar.google.com/citations?user=saEDGNAAAAAJ&hl=en/ Email: hamedsultani@uodiyala.edu.iq

Widyan Salman Abd Almahdy University of Diyala, Diyala, Iraq Email: drasatolia2020@gmail.com

Article submitted 2021-04-11. Resubmitted 2021-05-10. Final acceptance 2021-05-15. Final version published as submitted by the authors.