A Framework for Experience Based User Authentication Technique for Minimizing Risk of Brute-Force Attacks

Amirul I Mohamad, Mohamad A Mohamed, Mokhairi Makhtar, Mustafa Mamat, Norziana Jamil, Marina Md Din

Abstract: ***Authentication is the process of verifying somebody or something about who he claim he is. The current methods have some drawbacks, which is high cost for special tools, high maintenances, low reliability, lost or broken by user's poor handling and needs for special expertise in operating the system. In addition, brute force attack has been used against the authentication system by using special software readily available. To address this issue, we proposed an experience-based authentication system, which makes use of user experience as a password during the verification process. In this study, we choose a list of mountains climbed by a user in combination with the year of visit as a password. The system consists of two parts, sign up and sign in. User registration is done during the sign up, whereas user authentication is carried out during the sign in process. Given the number of mountains around the world that is nearly a million in total, and by allowing user to have any combination of mountain, the risk of brute force attack can be minimize significantly. The ability of this system that can withstand such an attack from the outside could increase the current standard security level.***

Index Terms: ***user authentication, experience based, knowledge based, brute-force attack.***

I. INTRODUCTION

Nowadays the society is highly depending on the internet for their everyday task. This is done by sharing their information with each other via the internet [1]. The information can be categorized into two namely the non-personal information and personal information. Some examples of non-personal information such as the weather forecast, news and those that are not related to specific person. The personal information is the information that can directly be related to the specific person [2], such as the identification number, address, phone number, username, and password. Without proper protection the data can be manipulated and thus put the owner in huge disadvantage. If the data is illegally owned by irresponsible person, it can be used to commit other criminal activities [3]. The activity of stealing data is normally done by black hat hacker.

Authentication has been the key to secure access to network. With the mushroom-like growth of different types of communication networks with different characteristics and requirements such as the satellite network [4], mobile network [5] and sensor network [6], authentication has becoming a much challenging area of research. By manipulating the vulnerability in the authentication system design, the attacker can manipulate and causing implicit damage to the compromise system. As a consequence, various types of user authentications [7] were used to authenticate the original user from an unauthentic one. In general, authentication can be categorized into two namely message authentication which normally get solved by using cryptography [8]-[10] and the other entity or user authentication, which is the interest of this study and also referred to henceforth.

The authentication prevents the attacker from easily accessing the user data. The authentication is making the attacker progress turn to time and resource consuming. It sometimes demotivates the attacker to continue the attack. Brute force is a type of attack that is used by the attacker to gain access to the targeted system by continuously trying the password combination until the correct password is obtained. Although it is seen as the weakest one, it is also the simplest one to execute against any authentications system.

In this paper, we propose a new breed of authentication method namely an experience-based authentication method to be used as a tool to safeguarding the sensitive data. One's experience can be very unique to an individual and therefore a suitable candidate for this task. As a proof of concept, we use data from user's experience as a password. Nevertheless, any type of other experience data can be used as a replacement.

This article is organized as the followed. Section 2 discusses the related works that has been done before in the domain of user authentication. Section 3 shows the proposed method that this paper highlighted and chapter 4 the conclusion of this paper.

Revised Manuscript Received on February 11, 2019.

Amirul I Mohamad, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, Malaysia.

Mohamad A Mohamed, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, Malaysia.

Mokhairi Makhtar, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, Malaysia.

Mustafa Mamat, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, Malaysia.

Norziana Jamil, Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia.

Marina Md Din, Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia.

II. RELATED WORKS

In the world where digital information is very valuable, the criminality trend has been shifted from physical attack to logical attacks. Logical attack can be very fruitful and much safer in that attacker does not require to physically being at the crime scene, in fact it can be mounted from anywhere in the world. This type of attackers is normally known as hackers and there are white hat hacker and black hat hacker. White hat hacker is a person or group of people that will search for weakness in system to improve the security of that system. On the other hand, black hat hacker is a person or group of people that misuse their expertise in hacking to find and manipulate the system weakness to proceed with unethical practice such as information steeling, information forging fraud and many more [3].

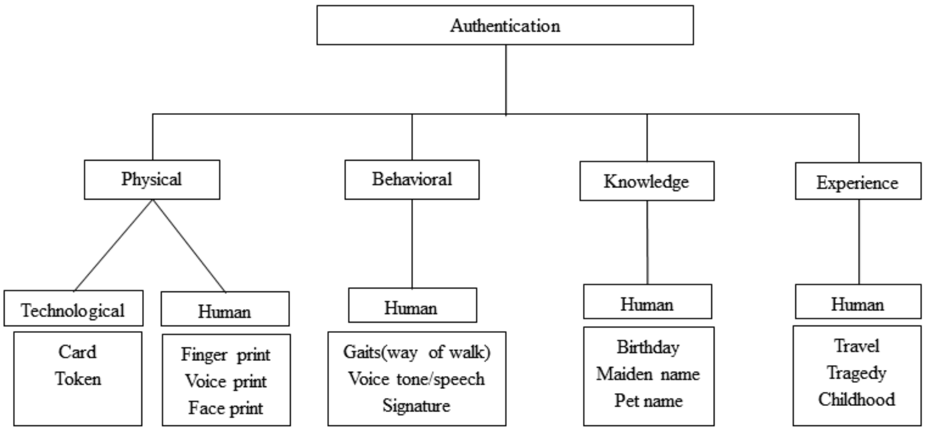

Fig. 1: Taxonomy of user authentication

Most of the user authentication process is highly depended upon the few commonly known approaches such that of physical based, behavioral based, and knowledge based as shown in Fig. 1. The physical based can be sub-categorized into that of humanoid and technological. The human physical considers all parts on the human body that can serve the authentication purposes, some examples are the fingerprint, voice tone, facial structure, human iris and retina. Whereas, the technological considers simple elements such as the smart cards and tokens which are simple and mobile enough to carry around unique information on particular entity or individual.

Fingerprint authentication is the process to differentiate someone identity based on the structure of one's fingerprint. The fingerprint can be interpreted as the pattern on the skin at the person fingertip. It is made of ridge pattern on the pad of finger. The clean and flat surface such as found on the glass is the easiest place to get the fingerprint pattern left behind. This happened because of the oily substance that is produced by human skin will cover every part of the surface simply [11], [12].

Human voice has served as a tool for short distance human communication between each other. It moves in the air in a form of frequencies. The ear converts these frequencies into the electrical impulses and then which later be translated by the brain. The brain is responsible to uniquely differentiate and recognize the speaker based on their voices. The same principle is used in the voice authentication method where the spectrogram is used to store the voice samples during the registration process. The verification process is quiet simple, the input received via the input device is recorded into the spectrogram. Then the comparison between the new voice data and the stored voice data is made. The result of the comparison will determine the validity of user identity.

Human can recognize somebody by looking at his or her face. It is because the face contains unique characteristics that make the identification is possible. These characteristics can be used in the face recognition technology that replicates the process of human recognizing somebody. The camera is use to record the face and the identification can start by calculating the distance ratio between the eyes, ratio eyes and mouth, forehead wideness and many more features that can be used as for identification [13].

The color ring around the eye pupil is called an iris. Its main function is to regulate the light quantity that enters the eye by expanding during the bright condition and retreat when in dark condition. The most importance feature of iris for use in the authentication method is the uniqueness of its color pattern and remains unchanged throughout a human life. The authentication method normally starts with the user registering the iris by recording it using a camera and then the distinct features are extracted and stored into a database. The authentication process starts with a user scanning the iris using the scanner and then searching for distinct features in the image. The comparison between the new and original data is done to determine the validity of user identity [14], [15].

The network of blood vessel in the eye is known as retina. It has a very unique pattern that will not be the same even for an identical twin. This trait makes it possible to be used for an authentication method. The authentication methods normally start with the user registering the retina by recording it using the camera and then the distinct feature is identified and stored into the database. The authentication process starts with user scanning the retina using the scanner

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

and then extracting for distinct features in the image. The comparison between the new and the original data is done to determine the validity of user identity [16]-[18].

The cards that contain chip or microprocessor are call smartcard. The information about user and card itself is stored inside the chip or microprocessor. The plastic is the main material normally use to make the card while the chip will sit under the gold plated rectangle contact on the card. To read the data from this card a special smartcard reader is needed. The smartcard is continuously improved to facilitate the increasing information of user [19].

The token is the small hardware which containing the information about a user. This device usually constructed using plastic. The information transfer is by using RFID (radio frequency identification). This device is embedded into an object that is used every day such as card, bracelet key mob and many more. The token is usually used as the additional factor for the two-factor authentication. In the two-factor authentication, the user will scan the token with the reader. The reader will communicate with the token and pulls the information needed from the token. Then, the system will ask the user to input the password or fingerprint corresponding to the information from the token [20], [21].

Meanwhile, the behavioral based authentication utilizes the unconscious human habits such as gaits, voice tone and signature. Gait is defined as the way of human walk. It is a part of the human behavioral. Every person has a unique way of walking making it is possible to exploit this behavioral to be a part of an identification process. To utilize this method, a user needs to have a device called accelerometer on the body to record the movement. Only recently, the motion detection camera has been introduced to the market and it can be used to replace the accelerometer for much better handling [22]-[24].

Voice tone can be defined as the way of someone saying something. The expression and emotion in saying the word in their native tongue will influence the word’s sound. Normally, foreigner’s pronunciation will not produce the same sound as that of the native speaker and therefore a good candidate for the use of authentication [25].

The product of streak on a surface is call a signature and it is a type of handwriting. It exists in different forms such as person’s name, symbol or a picture. Digital signature is no different to physical signature because of uniqueness it possessed thus be used for user authentication [26]-[28].

The knowledge based makes use of the information that is known to user but kept as a secret and mostly it is static. It will not change forever. Knowledge is the information that user already know. It can range from the private information to the generally known information that can be used for the authentication purpose. A user provides the information to the system during the registration process. To authenticate the user, the information inputted must be identical to information stored inside the database.

Challenge question method is a method that uses the question that has been register by a user into the system during the registration. To access the system the user need to answer the question that has been stored in the system. The answer must be the same with the system answer for system to grant access to the services [29], [30].

Cryptographic technique that allows the user to verify their identity is called Zero-knowledge proofs. It is made of the truth statements, and if the information is true, no related information is revealed. The interaction between two parties will have no new information. In general, this technique contains three properties. First, it should be soundness, meaning that is hard to fake the truth statements. Second, completeness, the user should provide the true statements every time and third is zero knowledge, no information is revealed to both parties if the statements is true [31].

Experience based is a new sub section from the taxonomy of user authentication. The experience is can be defined as an event that has been through personally by the user. The experience is used in many type of decision-making. The decision can be archived with or without the intervention from the third entity. In this study, a user is allowed to select 8 different mountains he used to climb together with the year of visit as a password. There exists more than a million of mountains worldwide, however for simplicity we take a subset of 1000 most famous mountains. In the next section we analyze how this number could affect the success of brute-force attacks.

III. PROPOSED FRAMEWORK

The proposed technique consists of two parts. They are registration and authentication. The registration part is to register the new user and the authentication part is to authenticate the registered user. The detail can be described following to Fig. 2.

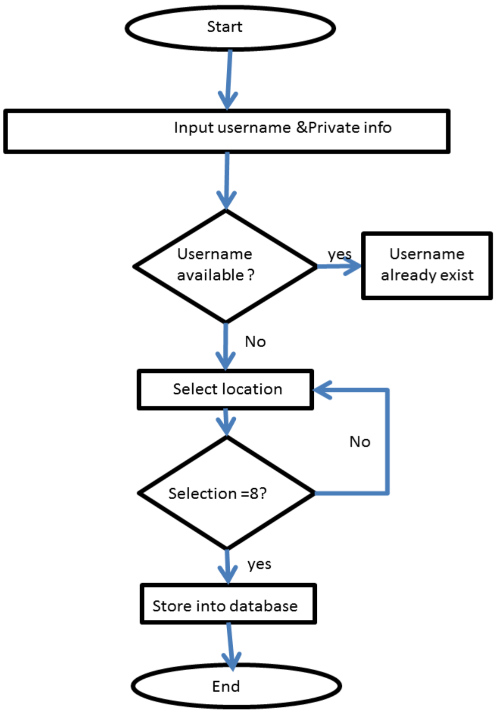

Fig. 2: Registration phase

In the registration phase, the user registers himself to the system's database. The registration process starts by asking user to input his personal information and the username that he wants to be recognized as by the system. The information will be saved into database. The user needs to select eight different mountains he has ever climbed together with the visit's year from the globe presented. The mountains' name will be stored inside the database together with the respective years.

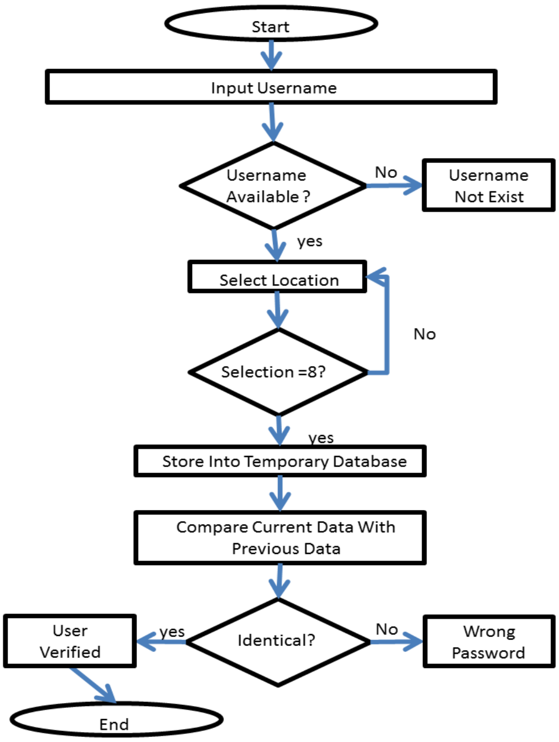

Fig. 3: Login procedure

In the login phase shown in Fig. 3, the process starts with the user will inputted the username and then clicked the next button. The username will be compared from database if the username exist user will redirect to the password imputed page. If there is no match, user will redirect to the registration page. Password input page will receive the password inputted by user and save temporarily inside the database. User need to select eight countries in ascending order by year identical when registration process. After the all inputted password is received .it will be compare with password that already stored inside database.

IV. RESULTS AND DISCUSSION

In this section, we use mathematical analysis to evaluate the strength of our technique to withstand brute-force attack. We are indebted to the principle of counting in the course of this analysis.

We claimed earlier that this system is designed to wisthand the brute force attack in that an attacker needs to allocate more time and energy into cracking the password. The permutation form $P = n^r$ where P = possible choices, n = total number of mountains, and r= number of mountains in password (should be at least 8), is used to evaluate this.

This formula is used when there are repetitions allowed, in other words user can choose the same mountain but different years. The number of trials needed to brute force this system can be calculated as follows.

Given the number of mountain that exist in the world is around 1 million, but in this paper we only consider a subset of 1000 mountains for simplicity. We limit the design to allow user to fixed number of input 8 mountains of his choice. From this figure, the number of probability for an attacker to try is $P = 1000^8 = 1\text{x}10^{24}$.Percentage of success can be calculated as $\left(\frac{1}{10^{24}}\right)\text{x}100 = 1\text{x}10^{-22}$. Using Intel Processor Core i5-6600K with the assumption of 11344618.21 computation per second, to brute force this system the average time taken can be calculated as $\frac{0.5\text{x}10^{24}}{11344618.21} = 283396101$ years. This number is sufficiently large to prevent the brute-force attack.

V. CONCLUSION

This paper proposed the authentication technique based on user experience that was shown to be able to prevent multiple brute-force attack from the unauthorized user. According to the mathematical analysis calculation, the time taken is more than a quarter billion years to success. This technique could be an alternative to current user authentication for future implementation.

ACKNOWLEDGMENT

The authors thank the Government of Malaysia for funding this research under the Fundamental Research Grant Scheme (FRGS/1/2018/ICT03/UNISZA/02/2) and also Universiti Sultan Zainal Abidin, Terengganu, Malaysia.

REFERENCES

1. P. Wei, and Z. Zhou, "Research on security of information sharing in Internet of Things based on key algorithm," Future Generation Computer Systems, 88, 2018, pp. 599-605.
2. D. Supriyadi, Personal and non-personal data in the context of big data. thesis, Netherlands: Tilburg University, 2017.
3. S. G. Langer, "Cyber-security issues in healthcare information technology," Journal of Digital Imaging, 30(1), 2016, pp. 117-125.
4. M. Rajanna, H. C. Kantharaju, and M. G. Shiva, "Satellite networks routing protocol issues and challenges: A survey," International Journal of Innovative Research in Computer and Communication Engineering, 2(2), 2014, pp. 153-157.
5. P. Gandotra, and R. K. Jha, "Device-to-device communication in cellular networks: A survey," Journal of Network and Computer Applications, 71, 2016, pp. 99-117.
6. B. A. Muzakkari, M. A. Mohamed, M. F. A. Kadir, Z. Mohamad, and N. Jamil, "Recent advances in energy efficient-QoS aware MAC protocols for wireless sensor networks," International Journal of Advanced Computer Research, 8(38), 2018, pp. 212-228.
7. L. Bonner, "Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches," Washington University Journal of Law and Policy, 40, 2012, pp. 157-177.
8. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, 21(2), 1978, pp. 120-126.

9. V. S. Miller, “Use of elliptic curves in cryptography,” Conference on the Theory and Application of Cryptographic Techniques, 1985, pp. 417-426.
10. M. A. Mohamed, “A survey on elliptic curve cryptography,” Applied Mathematical Sciences, 8(153-156), 2014, pp. 7665-7691.
11. H. Wimberly, and L. M. Liebrock, “Using fingerprint authentication to reduce system security: An empirical study,” IEEE Symposium on Security and Privacy, 2011, pp. 32–46.
12. D. Kumar, S. Singh, S. Pujari, and P. Mishra, “Fingerprint based attendance system using microcontroller and LabView,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 4(6), 2015, pp. 5111–5121.
13. F. Battaglia, G. Iannizzotto, and L. L. Bello, “A biometric authentication system based on face recognition and RFID tags,” Mondo Digitale, 13(49), 2014, pp. 1–17.
14. J. M. H. Ali, and A. E. Hassanien, “An iris recognition system to enhance e-security environment based on wavelet theory,” Advanced Modeling and Optimization, 5(2), 2003, pp. 93–104.
15. P. M. Shende, and M. V. Sarode, “Multiple biometric system application: Iris and fingerprint recognition system,” International Journal of Application or Innovation in Engineering and Management, 5(3), 2016, pp. 34–38.
16. K. Saraswathi, B. Jayaram, and R. Balasubramanian, “Retinal biometrics based authentication and key exchange system,” International Journal of Computer Appl., 19(1), 2011, pp. 1–7.
17. M. Sabaghi, “Retinal identification system based on the combination of Fourier and wavelet transform,” Journal of Signal and Information Processing, 3(1), 2012, pp. 35–38.
18. T. R. Borah, “Retina and fingerprint based biometric identification system,” Mobile and Embedded Technology International Conference, 2013, pp. 74-77.
19. M. Lapère, and E. Johnson, “User authentication in mobile telecommunication environments using voice biometrics and smartcards,” in Intelligence in Services and Networks: Technology for Cooperative Competition, A. Mullery, M. Besson, M. Campolargo, R. Gobbi, R. Reed, Eds. Berlin: Springer, 1997, pp. 437-443.
20. M. Singhal, and S. Tapaswi, “Software tokens based two factor authentication scheme,” International Journal of Information and Electronics Engineering, 2(3), 2012, pp. 383-386.
21. J. Payne, G. Jenkinson, F. Stajano, M. A. Sasse, and M. Spencer, Responsibility and tangible security: Towards a theory of user acceptance of security tokens. Available: https://arxiv.org/pdf/1605.03478.pdf.
22. T. Hoang, “On the instability of sensor orientation in gait verification on mobile phone,” 12th International Joint Conference on e-Business and Telecommunications, 2015, pp. 148–159.
23. P. Kaur, and G. S. Aujla, “Review on: Human identification using GAIT recognition technique with PAL and PAL entropy and NN,” International Journal of Computer Science and Information Technologies, 5(3), 2014, pp. 3281 – 3285.
24. S. Sprager, and M. B. Juric, “An efficient HOS-based gait authentication of accelerometer data,” IEEE Transactions on Information Forensics and Security, 10(7), 2015, pp. 1486–1498.
25. P. Gawali, and P. V. D. Jadhav, “Rhythm based authentication model: Towards secure and convenient authentication for mobile devices,” International Journal of Advanced Research in Computer Science and Software Engineering, 6(2), 2016, pp. 343–346.
26. J. Trevathan, and A. Mccabe, “Remote handwritten signature authentication,” 2nd International Conference on e-Business and Telecommunication Networks, 2005, pp. 335-339.
27. H. Srinivasan, S. N. Srihari, and M. J. Beal, “Machine learning for signature verification,” in Computer Vision, Graphics and Image Processing, P. K. Kalra and S. Peleg, Eds. Berlin: Springer, 2006, pp. 761-775.
28. A. Levi, and M. U. Caglayan, “The problem of trusted third party in authentication and digital signature protocols,” 12th Int’l Symp. on Computer and Information Sciences, 1998, pp. 317-324.
29. H. Fujii, and Y. Tsuruoka, “SV-2FA: Two-factor user authentication with SMS and voiceprint challenge response,” IEEE 8th International Conference for Internet Technology and Secured Transactions, 2013, pp. 283–287.
30. Y. Albayram, M. M. H. Khan, A. Bamis, S. Kentros, N. Nguyen, and R. Jiang, “Designing challenge questions for location-based authentication systems: A real-life study,” Hum. Cent. Comput. Inf. Sci., 5(17), 2015, pp. 1-28.
31. J. Kurmi, and A. Sodhi, “A survey of zero-knowledge proof for authentication,” International Journal of Advanced Research in Computer Science and Software Engineering, 5(1), 2015, pp. 494-501.