TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol.18, No.4, August2020, pp. 1998~2003
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i4.14898

Vulnerabilities detection using attack recognition technique in multi-factor authentication

Noor Afiza Mohd Ariffin[1], Fiza Abdul Rahim[2] , Aziah Asmawi[3], Zul-Azri Ibrahim[4]
[1,3]Faculty of Computer Science & Information Technology, University Putra Malaysia**,** Malaysia
[2,4]College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia

Article Info

Article history:

Received Aug 5, 2019
Revised Mar 3, 2020
Accepted Apr 13, 2020

Keywords:

Attack recognition
Efficiency
Multi-factor authentication
Security

ABSTRACT

Authentication is one of the essentials components of information security. It has become one of the most basic security requirements for network communication. Today, there is a necessity for a strong level of authentication to guarantee a significant level of security is being conveyed to the application. As such, it expedites challenging issues on security and efficiency. Security issues such as privacy and data integrity emerge because of the absence of control and authority. In addition, the bigger issue for multi-factor authentication is on the high execution time that leads to overall performance degradation. Most of existing studies related to multi-factor authentication schemes does not detect weaknesses based on user behavior. Most recent research does not look at the efficiency of the system by focusing only on improving the security aspect of authentication. Hence, this research proposes a new multi-factor authentication scheme that can withstand attacks, based on user behavior and maintaining optimum efficiency. Experiments have been conducted to evaluate this scheme. The results of the experiment show that the processing time of the proposed scheme is lower than the processing time of other schemes. This is particularly important after additional security features have been added to the scheme.

Corresponding Author:

Fiza Abdul Rahim,
Department of Computing, College of Computing and Informatics,
Universiti Tenaga Nasional,
43000 Kajang, Selangor, Malaysia
Email: fiza@uniten.edu.my

1. INTRODUCTION

Advancements and improvements of network infrastructures have brought the integration of electronic devices and information sharing which can be accessible by public. Security is in this manner a significant subject when it comes to information and data being shared [1, 2]. Security leads to the importance of secrecy and authentication. Secrecy is referred to protection of sensitive data against unauthorized access and modification. Rather, authentication is a mechanism to verify the identity of a user or process which helps to prevent unauthorized access to sensitive data [3, 4]. This research concentrates on authentication security and maintaining optimum efficiency. Security constraints in the authentication system must be placed at the highest level and must be a priority to consider in the development of a secure system [5, 6]. Based on system's specified permission, user authentication level will be determined [7-9]. Any authentication application involving public exposure or critical-business application requires a higher level of protection, especially against authentication attacks that may compromise hardware and/or data [10].

To compensate for the authentication process, various technologies have been developed to strengthen the weaknesses of specific objects and knowledge factor authentications [11, 12]. However, there are an increasing number of attacks that are related to authentication methods [2, 13-16]. Among the techniques developed to overcome this attack is attack recognition technique that can enhance security features to multi-factor authentication. The implementation of the attack recognition technique has been in existence for a long time and has also expanded over the past decades to include in the computer security domain, particularly in intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). This research incorporates a plan recognition technique of [17] as attack recognition into the authentication systems.

At the time of this research conducted, no other research had introduced attack recognition technique into authentication systems. This technique is widely used in intrusion detection systems (IDS), decision making and language understanding. For example, a new set of attack instances are identified to allow IDS able to detect possible new type of intrusion. In decision making system, attack recognition is used to analyze user action in order to determine their goal or result [18-20]. Based on the output, an appropriate response is proposed to the user.

In addition to security, authentication efficiency also emphasized on time taken. In a situation where there is high level of security, authentication process would take a longer time to verify a full message [21-23]. According to [17], efficiency is captured by measuring the time required to complete a task or the number of clicks or buttons pressed to achieve the required goal. Hence, a system is not only considered good by its functionality and level of protection, but it also must be efficient by enabling users to achieve their goal within a reasonable amount of time [24].

2. RESEARCH METHOD

2.1. Research method for security

In the authentication step, the overall process of the attack recognition technique is illustrated in Figure 1. Referring to Figure 1, the attack recognition receives data input from the user and observes the behaviours of the user regarding how it provides these data. This involves taking a series of observed user actions and matching them with examples of attacks available in the attack template database. The appropriate response will be given based on the matching result, as to whether the user is legitimate or a potential attacker. The entire process, starting from evaluating the user behavior, matching the action to known attacks in the database and providing the appropriate response or action, is carried out using the attack recognition technique.

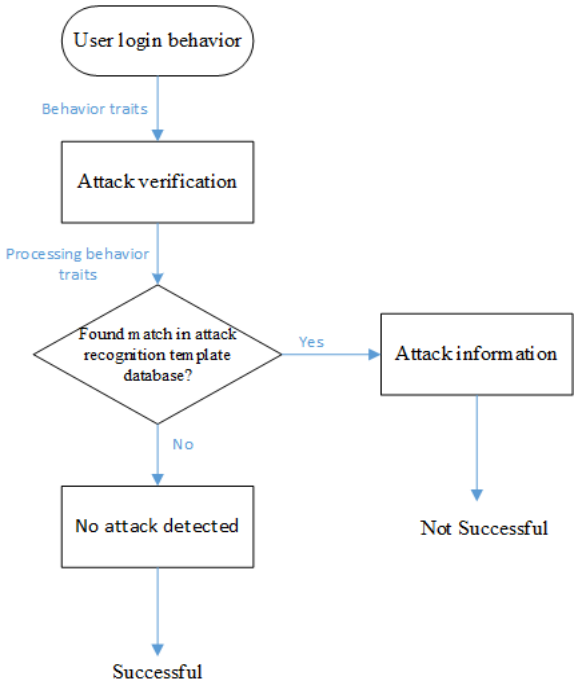

Figure 1. Attack recognition steps

In conventional authentication model, user identification is based on password, PIN or signature [25–27]. A user is detected by physical or behavioral features whilst in the biometric authentication system. Such features include fingerprinting, palm printing, eyes, iris, signature, voice, etc. In this study, the user input or information that is the user's username, face and fingerprint are compared during the matching process and must fit the data stored in the attack template database. The attack template database which is kept in the system's database contains all the information needed to identify and recognize an authorized user based on his user input. The database may be placed in a remote location or it can also be in the same location as the scheme. In the proposed scheme, the database sits in the same workstation as the scheme.

After the matching process is done, the system will give an appropriate message based on the result of the matching. If the user's action matches a template in the attack template database, the system will generate an error message (attack information), which explains the attack, the purpose of the attack, and the actions to solve the attack. If no match is found, the user will be considered legit and a message stating "No Attack Detected" will be shown and user will be allowed to proceed. The proposed scheme must recognize the true plan and intention of the user. The scheme should also respond appropriately to the user's actions. The role of detecting an intruder in web applications is even harder as the number of users on the internet is massive as compared to normal desktop applications. This research presents the security analysis that was done to test the proposed multi-factor authentication scheme to withstand attacks based on user attacks plan in the attack template database as shown in Table 1.

Table 1. User attacks plan

No.	List of Attacks
1.	Attempted Break-in
2.	Masquerading or Successful Break-in
3.	Intercepts by Unauthorized User
4.	Leakage by Illegitimate User

The user attacks plan consists of user action and user behavioral templates that the program will evaluate during the user login process. The proposed scheme was deliberately run by users under specific conditions in order to measure the proposed system level of security from user attacks. The user attack plan is aimed to provide an added layer to security by filtering out non-legitimate users who are attempting to break the system. Even if a user passes the initial steps of authentication (biometric and key generator), he or she might still be an attacker. The attack recognition will be able to analyze the user action and behavior during the user login process to determine if the user has any ill-intention. Since no previous researches has been conducted to apply user attacks in their schemes, no comparison will be made in the experiment.

In this experiment, 15 respondents involved to test the proposed scheme. The general steps involved in an experiment are listed below:

- All users are required to register themselves in the system.
- The user will try to log in and go through the authentication process.
- The user must follow the necessary steps to trigger the user attack plan during authentication process.
- Analysis of the results.

All respondents must follow the steps of the user attack plan as tabulated in Tables 2-5:

Table 2. Attack type: attempted break-in

	Steps	Condition Triggered	Action
1)	The user has a valid username.		
2)	The user does not have valid password.	3 continuous invalid logins	Username is highlighted as suspicious and details sent to the admin
3)	The user attempts to guess a random password.		

Table 3. Attack type: masquerading or successful break-in

	Steps	Condition Triggered	Action
1)	The user has a valid username.		
2)	Three-factor authentications (password, face, and fingerprint) is entered from different location (different IP address).	3 continuous login attempts but each login attempt are from different IP	Username is highlighted as suspicious and details sent to the admin
3)	The user successfully logs in.		

Table 4. Attack type: intercepts by an unauthorized user

Steps	Condition Triggered	Action
1. The user has a valid username. 2. The user successfully logs in to the 3-factor authentication. 3. The user keeps repeating login process in a short period of time.	3 successful logins within 1 minute	Username is highlighted as suspicious and details sent to the admin

Table 5. Attack type: leakage by illegitimate user

Steps	Condition Triggered	Action
1. The user has a valid username. 2. The user successfully logs in to the 3-factor authentication. 3. The user logs in at odd hours.	3 continuous successful logins	Username is highlighted as suspicious and details sent to the admin.

From the user attack plan above, each type of attack has different steps in determining the security level of the proposed scheme. The action reflects the appropriate response to user attack measures from the proposed scheme. The actions are given in accordance with the condition caused by this proposed scheme. Three attempts to log in to the scheme via the proposed scheme were given to respondents. The result from this proposed scheme is compared with two previous schemes from [11, 28]. Both of these studies were selected as their schemes have many similarities with the proposed scheme in terms of functionality and performance. Although other earlier research was considered for comparison, they did not use an algorithm, lack experimental methods or lack the data necessary to compare performance measurements. All 15 respondents are expected to successfully enroll in all 3 schemes first. This is to ensure the information of the user are maintained in the records of the system which will recognize the users as legitimate users. Figure 2 is the summary of the experiment done to measure the level of efficiency for all schemes.

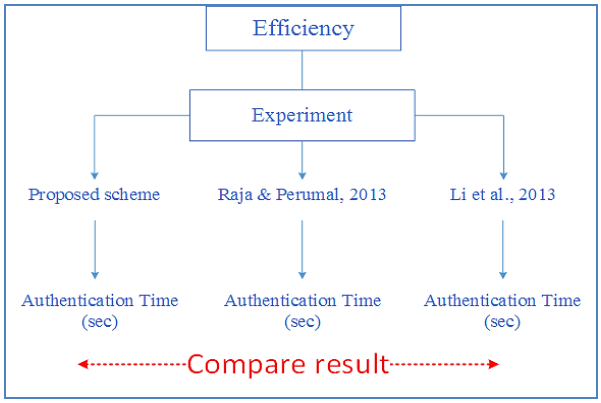

Figure 2. Summary of the experiment

3. RESULTS AND ANALYSIS

3.1. Result analysis for security

All 15 respondents carried out the four user attacks plan as listed in Table 1 to test the security level of the proposed scheme. As all respondents are required to follow the steps needed to trigger the user attack plan, the input is matched with template stored in the attack template database. The results show that the proposed scheme can withstand attacks and provide an appropriate response based on input from the respondents.

3.2. Result analysis for efficiency

It can be seen that the proposed time showed lower numbers, hence a shorter time to complete the task. Figure 3 shows the total time for all three logins done by the respondents in the experiment. From the result shown in Figure 3, not only the proposed scheme showed lesser time to execute the task, but it also showed almost similar processing time for all fifteen (15) recorded respondents. The previous scheme by [28] showed the second-best result. Finally, [11] took the longest time. Table 6 summarizes the experiment result based on average time in second for efficiency.

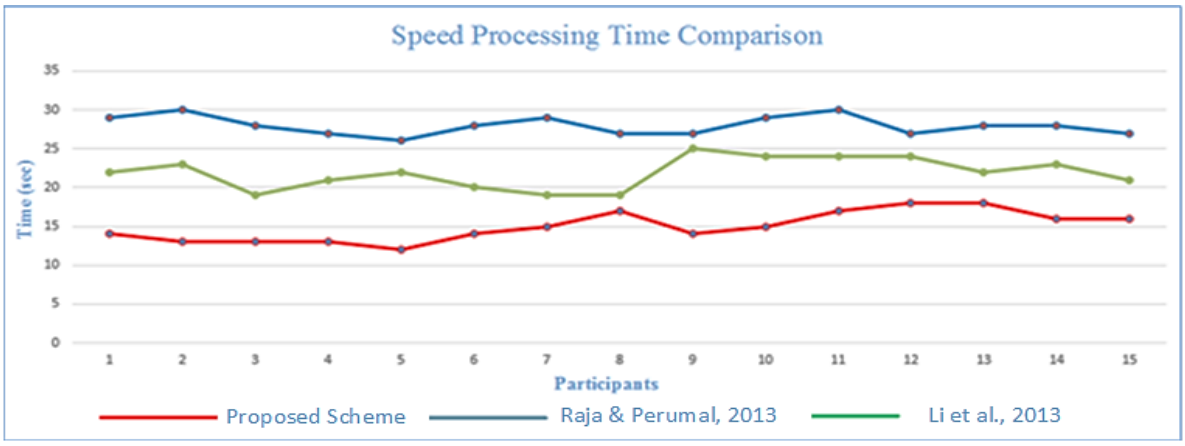

Figure 3. Total time taken all scheme

Table 6. Summary of result for three schemes

Rank	Scheme	Average Time (sec)
1	Proposed Scheme	15
2	Li et al [28]	21
3	Raja & Perumal [11]	28

4. CONCLUSION

This proposed scheme serves as a scheme to authenticate users on any application via the execution of attack recognition technique along with a biometric matching process. This is done by matching the input from the user with a template stored in the database. Additionally, this research integrates the attack recognition process to detect potential impostors based on the observed impostor actions. The attack recognition is able to forecast the impostor actions and provide a suitable response based on their actions.

This research also measured the level of efficiency of the scheme based on the speed of processing time. The time starts on the user login until their success in accessing the system. This research through the result of its experiment has proven to be faster in processing time compared to the previous schemes. This research performed better in terms of efficiency when compared to the previous schemes by Raja & Perumal [11] and Li, et al [28]. The previous scheme by Raja & Perumal [11] were having high processing time during the random number generator step. The random number was sent to the mobile user phone which was on a different network which is GSM, which then contributed to higher processing time. On the other hand, previous research by Li et al. [28] used a robust biometric multifactor which is called elliptic curve cryptosystem. This technique was aimed to provide higher security levels to the system but contributed to higher processing times. Based on the experiment results, the proposed scheme was able to achieve the results even with all its integrated security features. With the increasing number of attacks and intrusions on the authentication system, it is important to keep them secured and executable in a reasonable amount of time without having to delay the processing time.

REFERENCES

[1] A. A. Bakar, A. A. Ghapar, and R. Ismail, "Access control and privacy in MANET emergency environment," *2014 International Conference on Computer and Information Sciences (ICCOINS)*, 2014, pp. 1–6.
[2] Symantec, "Internet Security Threat Report: Volume 23," 2018.
[3] J. Malik, D. Girdhar, R. Dahiya, and G. Sainarayanan, "Reference Threshold Calculation for Biometric Authentication," *Int. J. Image, Graph. Signal Process.*, vol. 2, pp. 46-53, 2014.
[4] C. Liu, G. D. Clark, and J. Lindqvist, "Where Usability and Security Go Hand-in-Hand: Robust Gesture-Based Authentication for Mobile Systems," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 374–386, 2017.
[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition," *Computer Science*, 2009.
[6] U. Shafique, et al., "Modern Authentication Techniques in Smart Phones: Security and Usability Perspective," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, 2017.
[7] C. H. Liu, Y. F. Chung, T. S. Chen, and S. De Wang, "The enhancement of security in healthcare information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1673–1688, 2012.

[8] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things : threats and challenges," *Secur. Commun. Networks*, 2013.
[9] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review.," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–62, Jun. 2013.
[10] A. Nigam and P. Gupta, "Designing an accurate hand biometric based authentication system fusing finger knuckleprint and palmprint," *Neurocomputing*, vol. 151, pp. 1120-1132, 2015.
[11] A. Y. Raja and S. A. Perumal, "Effective Method of Web Site Authentication Using Finger Print Verification," *Int. J. Comput. Electr. Eng.*, vol. 5, no. 1, pp. 545-548, 2013.
[12] S. H. Khan, M. Ali Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," *Pattern Recognit.*, vol. 48, no. 2, pp. 458-472, 2015.
[13] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019.
[14] A. Gupta, A. Anpalagan, G. H. S. Carvalho, A. S. Khwaja, L. Guan, and I. Woungang, "Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey," *J. Netw. Comput. Appl.*, vol. 132, pp. 118–148, 2019.
[15] A. Iqbal, F. Mahmood, A. Shalaginov, and M. Ekstedt, "Identification of Attack-based Digital Forensic Evidences for WAMPAC Systems," *Proceedings-2018 IEEE International Conference on Big Data, Big Data 2018*, pp. 3079–3087, 2019.
[16] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, 2019.
[17] N. F. M. Sani, N. A. M. Ariffin, and R. Atan, "Design of object-oriented debugger model by using unified modeling language," *J. Comput. Sci.*, vol. 9, no. 1, pp. 1-29, 2013.
[18] C. So-In, N. Mongkonchai, P. Aimtongkham, K. Wijitsopon, and K. Rujirakul, "An evaluation of data mining classification models for network intrusion detection," *2014 4th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2014*, 2014.
[19] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Comput. Networks*, 2019.
[20] N. Tsinganos, P. Fouliras, G. Sakellariou, and I. Mavridis, "Towards an automated recognition system for chat-based social engineering attacks in enterprise environments," *ACM International Conference Proceeding Series*, 2018.
[21] S. Chaudhary, "The Use of Usable Security and Security Education to Fight Phishing Attacks," Thesis for: PhD Computer Science, Advisor: Eleni Berki, Marko Helenius, Markku Turunen, University of Tampere, 2016.
[22] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," *Proc.-12th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGrid 2012*, pp. 556–563, 2012.
[23] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," *Comput. Networks*, vol. 102, pp. 83–95, 2016.
[24] R. Kainda, I. Flechais, and A. W. Roscoe, "Security and usability: Analysis and evaluation," *ARES 2010-5th Int. Conf. Availability, Reliab. Secur.*, pp. 275–282, 2010.
[25] B. R. Naidu, K. V. L. Bhavani, C. Someswara Rao, and P. V. G. D. Prasad Reddy, "Comparative analysis of three single trait biometric authentication models," *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019*, 2019.
[26] C. J. Gibson and K. J. Abrams, "Will Privacy Concerns Derail the Electronic Health Record? Balancing the Risks and Benefits," *Healthcare and the Effect of Technology*, IGI Global, pp. 178–196, 2010.
[27] S. Saxby, "The 2013 CLSR-LSPI seminar on electronic identity: The global challenge-Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11–15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand," *Comput. Law Secur. Rev.*, vol. 30, no. 2, pp. 112–125, Apr. 2014.
[28] X. Li, J. Niu, M. K. Khan, J. Liao, and X. Zhao, "Robust three-factor remote user authentication scheme with key agreement for multimedia systems," *Secur. Commun. Networks*, vol. 9, no. 13, 2016.