ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURED AND EFFICIENT MULTI-FACTOR BIOMETRIC AUTHENTICATION SCHEME USING PLAN RECOGNITION TECHNIQUE

[1]NOOR AFIZA MOHD ARIFFIN, [2]NOR FAZLIDA MOHD SANI, [3]ZURINA HANAPI, [4]RAMLAN MAHMOD

[1,2,3,4]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), 43400 Serdang, Selangor, Malaysia.

E-mail: [1]afiz_efy@yahoo.com , [2]fazlida@upm.edu.my, [3]zurinamh@upm.edu.my , [4]ramlan@upm.edu.my

ABSTRACT

One of the most important parts in security is an authentication. It has become an essential security features for network communication. Nowadays, there is a need for strong level of authentication to ensure high level of security is being delivered to the application. All of this being done while still maintaining the desired level of performance that is expected of it. However, this approach brings challenging issues on efficiency and security. There have been several schemes and proposals related to multi-factor authentication previously but all of these schemes are still vulnerable to certain types of attacks. Furthermore, a more pressing issue for multi-factor authentication is on the high execution time which leads to a downfall in overall performance. The objective of this research is to propose an authentication method scheme and measure the effectiveness based on the authentication time. This scheme uses plan recognition technique, which is able to detect and identify the user effectively, defend from well-known attacks such as brute force or dictionary attack. The proposed scheme should able to run with a very low execution time. An experiment has been conducted to evaluate the scheme. Result from the experiment shows that the proposed scheme processing time is lower than the other previous schemes. This is even after additional security features has been added to the scheme.

Keywords: *Multi-Factor Authentication, Biometric, Plan Recognition, Effectiveness, Execution Time*

1. INTRODUCTION

More computers and network devices have been collaborating together due to rapid development of network facilities. This process involves exchanging a great amount of information to meet user demands. Hence, security becomes an important role to maintain the integrity of data being transferred over. Basically, in network security have two types of requirements, which is secrecy and authentication. Secrecy protects sensitive data from modification and eavesdropping, whereas authentication prevents data from forging and illegitimate of network access. For years, identity authentications in computer systems are based on keys, PIN or password. The most common scheme is the passwords usage. The usage of password authentication has been used in many applications until today due to easy to use, easy to implemented and is also by far the cheapest option. However, the use of password has a major drawback. It is easily forgotten. Meanwhile the use of physical security objects such as keys or smart cards likely to be stolen or lost. Because of these constraints, there is a need to put high priority in creating a more robust authentication method. Authentication can be considered one of the main fundamentals in building-up a secure system. A good and effective authentication method should allow needs being required and restrict need based on system request.

The use of biometrics technology provides a strong and effective way to counter all current authentication security shortcomings. In the technological era today, machines will replace almost every aspect of human life. Biometrics is able to utilize several surveillance techniques to the benefit of the user. To achieve a higher identification percentage in authentication, biometrics should be combined with something that uniquely expresses the given person. Biometrics offers schemes to verify the identity of person by using human physical traits such as fingerprint or face. Although biometric techniques are considered more secure if compared to other techniques, they are still open to vulnerabilities such as spoofing attack. This is because most biometric deployment in the real world uses single factor authentication. Some of the problem of single authentication method such as security in privacy information may be overcome by using multi-factor authentication scheme that integrates multiple factors of authentication.

As authentication the gate way to any secure system and it is evolve with time, it is mandatory for security procedure to always update so that the users can continue enjoy the benefits with fast access without being concerned about any sort of threats. However, the problem of efficiency and speed processing time in large scale authentication system which is cannot be solved fundamentally is still remained. It is very significant for matching data in large scale system which have a hundreds of millions data. As the increase in scale demands, a higher level of efficiency and speed is greatly needed.

The aim of this research is to introduce a new multi-factor authentication scheme framework by using biometric technology. The newly proposed scheme framework should be able to withstand any harmful security vulnerabilities accurately and efficiently.

The remaining of the paper is organized as follows. We first summaries related work in Section 2 and we introduce our methodology applied in this research in Section 3. We summaries the evaluation of efficiency on proposed multi-factor authentication scheme in Section 4. In Section 5, some experiments are discussed and the results are presented to show the performance of proposed scheme in term of speed processing time. Finally, presents the conclusions of the research work carried out and points out several of recommendations for future works for exploration and open problems that have been discovered throughout the tenure of this research.

2. RELATED WORK

2.1 Plan Recognition Technique

The implementation of plan recognition in computer security has been known for decades especially in the use of intrusion detection system (IDS). However, previous researches have never implemented plan recognition techniques in authentication systems. Normally, plan recognition is implemented in language understanding, intrusion detection system, or attack recognition to identify attackers and so on. The existing intrusion detection system (IDS) system does not predict future attacks and also does not provide any early warning when an attack is taking place. In a research done by [1], present plan recognition in intrusion detection system (IDS) meets the needs of network security domain. According to this research, the intrusion detection system (IDS) must cooperate with artificial intelligence method for the plan recognition to be more effective and proactive. The limitation of this research only focuses on the need of plan recognition to solve problems in network security and this research still does not provide a facility to represent that agent maybe engaging in actions solely to mislead the observer.
Another research done from [2] applies plan recognition by correlating or analyzing security alerts with the attack scenario and gives a fit response. They conduct a probability of inference which related and analyze the attack scenario and introduce a technique to solve three problems. First, they will simulate attack scenario come from recorded low level alert correlation. Second, they will recognize the attacker's attack plan. Third, they make some predictions on potential future attacks based on past observations. This research only focuses on low level of alert correlation. The limitation of this approach is built attack plans built attacks plan on security experts' knowledge and understanding of networks and systems under protection in attack plan recognition. These researches also not distinguish the deceptive plan and the real goal of the attackers.

2.2 Multi-factor Authentication

The increasing numbers of application with needs of authentication along with the development of attacks has called to multi-factor authentication approach. Multi-factor authentications are considered stronger authentication compare to single-factor authentication as they combine several of the authentication factors.
The proposed authentication scheme by [14] has provided an enhanced security with an optimal overall time taken for the operation. The proposed scheme use the biometric data embedded in a smart card together with the username and password of the user. Their research also compared the time performance with existing Secure Socket Layer based authentication scheme and attacks which the proposed scheme is able to withstand. This research claims that their scheme has provide a time efficient authentication, however, their scheme is

still have increasing time during registration and have a heavy weight encryption algorithm.

According to the research from [19] it proposes a new scheme which features fingerprint images extraction. This proposed method is not efficient because it still has a high execution time. Hence, it cannot be acceptable for commercial use. In order to be acceptable for commercial use, the execution time of the proposed algorithm must be substantially reduced.

Research from [20], describes the prototype of authentication by using fingerprints to authenticate the identity of a person. This research need to make some improvement on minutiae-extraction algorithm to be faster in term of response-time and more accurate.

Research [21] applied GA for fingerprint matching. This researchers' claims that their scheme has provided an efficient authentication; however, their scheme still has a high execution time.

Recently, research from [22] introduce the remote user authentication scheme with flexible biometric. It is using an El Gamal's cryptosystem and fingerprint. This research not uses a verification tables on the server. This research states that their scheme is more secure from attacks and very suit to applications which need high security. Based on paper reviewing, this research is still vulnerable to attacks and it can be easily to be cryptanalyzed.

Based on the research from [23], it is not efficient in communication and computational cost. This is because of the introduction of a 1024-bit password which is very difficult for users to memorize. Moreover, Research from Hwang and Li's use a discrete algorithm problem. It is based on difficulty of this algorithm, when the discrete algorithm problem is solved, it become insecure.

Table 1 Capability of Existing Research

	Authentication Scheme	Security Features	
		Efficiency	Security
1.	N. Ratha et al., 1995	×	-
2.	Jain , et al., 1997	×	✓
3.	Tan and Bhanu, 2006	×	-
4.	Gnanaraj, J. W. K., et al, 2013	×	-
5.	Lin-Lai, 2004	×	✓
6.	Bhargav - Spantzel et al, 2006	-	✓
7.	Lee & Liu et al. 2009	✓	-
8.	Hwang and Li,2000	×	×
9.	Proposed Scheme	✓	✓

3. METHODOLOGY

The research is conducted with a methodology which consists of 3 steps as shown in Figure 1, and the descriptions are as the following.

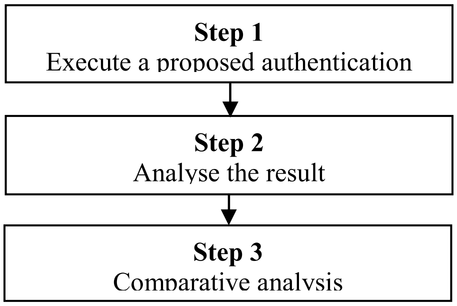

Figure 1: Research Methodology Steps

Step 1: User registration and execution of the authentication scheme

Users will first need to register to the proposed scheme. The factors needed are the users' username, fingerprint and face. Upon successful registration, users will need to login to the system by using the proposed authentication scheme. Each user will be given 3 login attempts. Time (in seconds) will be recorded for each successful login to measure the effectiveness of the scheme. This will be referred as the execution time

Step 2: Analysing the result

After all users have tested the proposed scheme, all execution time statistics from the users will be analysed. The measured time will be in seconds. Measured execution time will be the accumulative time from when user inputs in their details, the scheme interacts with the database and finally until the result is shown. Detail layout in graph form will be presented to show a more linear pattern for execution time representing statistics from all the users.

Step 3: Comparative Analysis

In this step, the obtained result for step 2 will be compared with previous published researches. This comparison is done manually.

4. EVALUATION OF EFFICIENCY OF PROPOSED SCHEME

One case study was done to evaluate this proposed scheme. It consists of respondent students from Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM). The research case will follow the steps in the validation process as below.

1. The user needs to register with the system whenever a new account is created.
2. To run the authentication process, they need to login into the system.
3. Record the time they complete the authentication tasks as results.
4. The result of the cases will act as a guideline to evaluate the efficiency of the scheme.
5. The results from this research will be compared with previous research.

This research has conducted an experiment to validate the use of the proposed scheme. This research analyzes the usage of proposed multi-factor authentication schemes in two different scenarios. The first scenario was developed as a basic authentication scheme, namely without security features. For the first scenario of authentication scheme, this research had developed a scheme that not integrates with security features like plan recognition and secure key technique. This is a traditional multi-factor biometric authentication scheme which only contains a username, password, face and fingerprint factors. Another second scenario has been added with security features such as plan recognition and secure key. Mean that, this scheme that was developed has been enhanced by integrating security features, namely plan recognition and secure key based on key generator technique. In the experiment, the proposed scheme will be compared with previous scheme which developed by [15]. They uses a combination of cued click point graphical password method along with the one-time session key to achieve higher security and better usability levels. The proposed scheme and a previous scheme uses a different technique in security authentication; the propose scheme use a plan recognition and secure key that generates from key generator technique while the previous scheme uses cued click point graphical password technique along with the one-time session key technique. Both schemes are multi-factor biometric authentication scheme.

In order to evaluate the efficiency of the proposed scheme, sixty (60) respondents known as students from Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM), are selected to participate in the experiment. Our experiment consisted of a user study conducted in a laboratory. The respondents were divided randomly into two groups with thirty (30) respondents for each group. One group represents the type of scheme without security features while another group is representing the multi-factor authentication scheme that includes security features. The respondent from both groups required to create their own username before register into the scheme. This is to ease and accelerate the registration process. There have three login sessions after the enrollment session. So, they have to run the scheme separately as three time login. The experiment was conducted separately for each group. One of the objectives of this research is to measure the efficiency of the proposed scheme in authentication. The efficiency is based on the time that the users take the input, compare with database and produce the results in unit second (sec).

5. RESULTS AND DISCUSSION

The results from the experiments are shown in the figures below. Based on the figure below shows the graphs the result from the proposed scheme between previous scheme, it is shown the speed processing time proposed scheme is faster than the speed processing time for previous scheme. Although this proposed scheme have been added with security features, it still can provide a low speed processing time than the previous scheme.

The figure 1 is the corresponding chart for previous scheme by [15], it is clear to show that the speed processing time taken for the first time login is much higher than the second and third login. However, when compared the time with the proposed scheme, it is proved that our proposed scheme, whether integrated with security or not is much lower than the previous scheme. The corresponding graph is shown in figure 2 is about the proposed scheme integrating with security features. The graphs also give the average time taken for the user to complete the authentication process. While figure 3 below, it shows the graph for speed processing time and average for the proposed scheme without security features. Both graph in figure 2 and 3 shows that the speed processing time taken for all attempts is much lower than the previous scheme. It is also shows that the speed processing time taken for all attempts is irregular since the users convenient in using the scheme due to demonstration is carried out before experiment started.

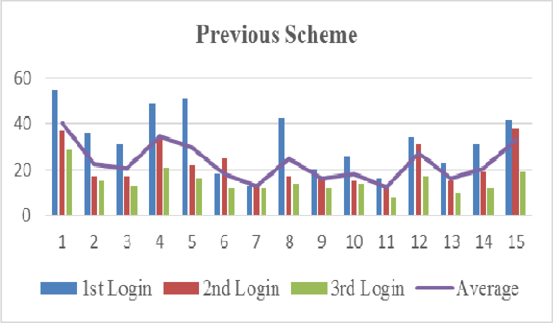

Figure 1 Speed Processing Time From Previous Scheme

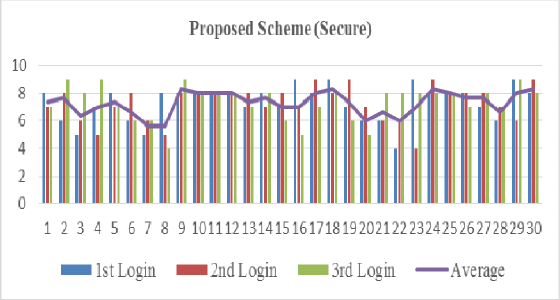

Figure 2 Speed Processing Time From Proposed Scheme Integrated With Security Features

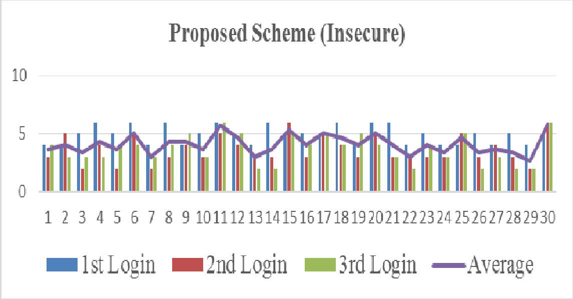

Figure 3 Speed Processing Time From Proposed Scheme Without Security Features

Based on the corresponding figure 4, it shows the comparison of average of speed processing time between three schemes which is previous scheme, proposed scheme integrated with security features and proposed scheme whereas not integrated with security features or known as traditional multi-factor authentication scheme. The previous scheme from the first attempt login is needed around average of 35 second while secure proposed scheme, the average is 9 second and insecure proposed scheme is need 5 second in average. There are some features that have been compared in this research, such as the time taken all along the authentication process to use a different techniques and different level of security.

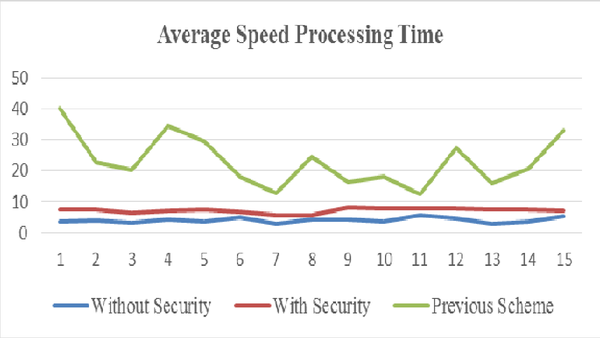

Figure 4 Average Of Speed Processing Time

6. CONCLUSION AND FUTURE WORK

This research proposes a multi-factor authentication scheme which integrates three factors such as password, fingerprint and face which this combination has never been used before in any previous research. Other than multi-factor, the proposed scheme also integrates plan recognition technique which can detect, identify and help to authenticate users in the network. The proposed scheme is able to achieve its goal with a low execution time result which is not supported by any of the previous schemes. In addition, this paper does performance comparison with some existing schemes to prove that this research is indeed able to deliver such low execution time. Furthermore, this proposed scheme can withstand popular vulnerability attacks such as brute force or dictionary attacks.

Although the research accomplished its main objectives, some issues remain that must be addressed and new paths for research must be discovered. The future work for this research is necessary to evaluate the usefulness of this research by using a dataset from well-known database such as from NIST dataset. In authentication phase after the scheme verify the username with database, this research will generate secure key and send to user via email. Apart from using email, this research could also use a mobile network to send a secure key to the authorized user.

ACKNOWLEDGEMENTS

Special thanks from authors for financial support from University Putra Malaysia.

REFRENCES:

[1] Geib, C. W., & Goldman, R. P. (2001). Plan recognition in intrusion detection systems. In *DARPA Information Survivability Conference &amp; Exposition II, 2001. DISCEX'01. Proceedings* (Vol. 1,

pp. 46-55). IEEE.

[2] Qin, X., & Lee, W. (2004, December). Attack plan recognition and prediction using causal networks. In *Computer Security Applications Conference, 2004. 20th Annual* (pp. 370-379). IEEE.

[3] Jarvis, P. A., Lunt, T. F., & Myers, K. L. (2005). Identifying terrorist activity with AI plan recognition technology. *AI Magazine*, *26*(3), 73.

[4] Chen, G., Yao, H., & Wang, Z. (2010, January). An intelligent WLAN intrusion prevention system based on signature detection and plan recognition. In *Future Networks, 2010. ICFN'10. Second International Conference on* (pp. 168-172). IEEE.

[5] Blythe, J., Camp, J., & Garg, V. (2011, February). Targeted risk communication for computer security. In *Proceedings of the 16th international conference on Intelligent user interfaces* (pp. 295-298). ACM.

[6] Wang, L. (2015). Research of Artificial Intelligent Plan Recognition Method in the Multi-Agents Conditions.

[7] M. R. (2011). What is single-factor authentication (SFA)? - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA

[8] O. L. (2011). What is single-factor authentication (SFA)? - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA

[9] Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., & Ross, A. (2004, August). Biometrics: a grand challenge. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on* (Vol. 2, pp. 935-942). IEEE.

[10] Kaur, D., & Talwar, M. Analysis of Enhanced Multimodal Biometrics System for Speech & Signature using Noisy Samples

[11] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, *40*(3), 614-634.

[12] Huang, Y., Huang, Z., Zhao, H., & Lai, X. (2013). A new one-time password method. *IERI Procedia*, *4*, 32-37.

[13] Sadi, M. S., & Kanij, T. (2013). Fingerprint verification: A comparison of three approaches. In *Defense Science Research Conference and Expo (DSR), 2011* (pp. 1-5). IEEE.

[14] Gnanaraj, J. W. K., Ezra, K., & Rajsingh, E. B. (2013). Smart card based time efficient authentication scheme for global grid computing. *Human-centric Computing and Information Sciences*, *3*(1), 1-14.

[15] Mathew, G., & Thomas, S. (2013). A Novel Multifactor Authentication System Ensuring Usability and Security. *arXiv preprint arXiv:1311.4037.*

[16] A. Rattani, D. R. Kisku, M. Bicego, Member, IEEE and M. Tistarelli, "Feature level fusion of face and finger Biometric," 2013

[17] Kiruthika, R. & Prof. B. Rajesh Kumar M.E. (2014). Combination of Fingerprint for Security Protection, International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 5.

[18] Nigam, A., & Gupta, P. (2015). Designing an accurate hand biometric based authentication system fusing finger knuckleprint and palmprint. *Neurocomputing*, *151*, 1120-1132.

[19] Ratha, N., Chen, S., and Jain, A. K. (1995) "Adaptive flow orientation based feature extraction in fingerprint images," *Pattern Recognition,* vol. 28, no. 11, pp. 1657–1672,

[20] Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9), 1365-1388.

[21] Tan, X., and Bhanu, B. (2006) "Fingerprint matching by genetic algorithms," Pattern Recogn., vol. 39, pp. 465–477.

[22] Lin, C. H., & Lai, Y. Y. (2004). A fingerprint-based user authentication scheme for multimedia systems. In *Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on* (Vol. 2, pp. 935-938). IEEE.

[23] Hwang, M. S., & Li, L. H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, *46*(1), 28-30.

[24] Ratha, N., Chen, S., and Jain, A. K. (1995) "Adaptive flow orientation based feature extraction in fingerprint images," *Pattern Recognition,* vol. 28, no. 11, pp. 1657–1672,