Global Journal of Engineering and Technology Review

Journal homepage: www.gjetr.org

Global J. Eng. Tec. Review 3 (4) 10 – 18 (2018)

A Multi-Factor Authentication Scheme Using Attack Recognition and Key Generator Technique

[*]Noor Afiza Mohd Ariffin [1], Noor Fazlida Mohd Sani[2]

[1]Department of Computer Science, Faculty of Computer Science and Information Technology, 43400, Serdang, Malaysia

[2]Department of Computer Science, Faculty of Computer Science and Information Technology, 43400, Serdang, Malaysia

ABSTRACT

Security plays an important role in many authentication applications. Modern era information sharing is boundless and becoming much easier to access with the introduction of the Internet and the World Wide Web. Although this can be considered as a good point, issues such as privacy and data integrity arise due to the lack of control and authority. For this reason, the concept of data security was introduced. This research was focused on the authentication of data security. There have been substantial research that discusses on multi-factor authentication scheme but most of those researches do not entirely protect data against all types of attacks. Most current research only focuses on improving the security part of authentication while neglecting other important parts such as the accuracy and efficiency of the system. Current multifactor authentication schemes were simply not designed to have security, accuracy, and efficiency as their focus. To overcome the above issue, this research will propose a new multi-factor authentication scheme, which is capable to withstand external attacks, which are known security vulnerabilities, and attacks, which are based on user behaviour. On the other hand, the proposed scheme still needs to maintain an optimum level of accuracy and efficiency. From the result of the experiments, the proposed scheme was proven able to withstand the attacks due to the implementation of the attack recognition and key generator technique together in the proposed scheme.

Type of Paper: Empirical

Keywords: Security, multi-factor authentication, biometric.

1. Introduction

In today's world, the ever changing and improvement of network facilities has brought more electronic devices together where information and resources are shared and openly accessible to anyone who seeks it. Therefore, security has become an important subject when dealing with shared information and data. Security can be categorized into two, which are secrecy and authentication. Secrecy is a protection of sensitive data against unauthorized and unwanted eavesdropping and modification. On the other hand, authentication is a mechanism that helps

[*]Paper Info: Revised: August 13, 2018

Accepted: December 18, 2018

[*]Corresponding author: Noor Afiza Mohd Ariffin

E-mail: noorafiza@upm.edu.my

Affiliation: Faculty, University Putra Malaysia

to prevent any unwanted forgery and unauthorized access to sensitive data. Thus, the subject of this research is to focus on the security of the authentication process. Security constraints should be incorporated at the highest level in an authentication scheme. Security will be the top priority to be considered in the process of building up a secure system. It reflects the fact of whether or not the authentication level of a user should be allowed or restricted based on the permission defined in the system. There are three different types of factors that can be used for user authentication. The first would be a knowledge factor, which could be a password or PIN. Object factor, the second factor that could be a card with a magnetic strip or the use of a smart card. The third factor, which is a biometric factor, could be the use of physical features such as face imaging, human fingerprints, or human behavioural traits for example user signature. The most common authentication scheme is the use of a password that is grouped under the knowledge factor, which has also been the most prevalent factor for authentication in the last couple of decades. Most users can easily choose to remember passwords such as their own name or birth dates, the name of their pets, or the use of any common words. There have been many occasions that even by applying strong passwords on your system, the password can also be hacked by a determined intruder. On the other hand, if too many restrictions are imposed to create a strong password, it may affect users as they can easily forget their own password.

However, recent security breaches have shown that the use of single-factor authentication (SFA) mechanisms are insufficient (Dragusin, 2013). Security threats against poorly protected authentication mechanisms are constantly increasing (Khan et al, 2015). Due to the problems and shortcomings of single-factor authentication mechanisms, many have turned their heads to the use of multi-factor authentication (MFA). MFA will be the mechanisms taken by industry leaders and academic researchers.

Any application of authentication, which includes exposure to the computing environment, requires a higher level of protection, especially from vulnerable attacks that can compromise a user's identity or undermine the security of computer hardware and/or data. Other than security, the efficiency of authentication also needs emphasis, especially in terms of time. This is because an authentication scheme, which has a high level of security, will take a longer time for a complete message to be authenticated. Authentication has attracted much attention, as a form of technology to compensate for certain weaknesses of objects and knowledge factor authentications. With the widespread adaptation of the computing environment, the scope of authentication has been extended to include a broader area, and the number of users that use authentication schemes has increased exponentially, especially in biometric authentication. Indirectly, the accuracy of user authentication becomes an important due to the increase in the number of users.

Biometrics provides a strong user authentication solution. In the rapid technological development of today, machines are replacing every aspect of human life. Therefore, the security concern is paramount and there is a need to increase the automation of different surveillance techniques and authentication of users. To achieve a more secure authentication, the process should be combined with something unique that the authorized person has. Human biometrics is the use of human characteristics. Combining biometrics with the traditional use of passwords to create a functional and highly secure multi-factor authentication (MFA) mechanism. In recent years, biometrics technology has greatly improved and has clearly reached a matured level. However, one area in biometrics, which is the biometric templates for storage and communication, still poses a challenge. Biometrics offers automated schemes of identity verification based on human physiological or behavioural aspects such as face, fingerprint or voice sample. Furthermore, the characteristics measured in biometrics must be unique. Although biometric techniques are more secure compared to other techniques of authentication, these methods are still open to vulnerable attack because most authentications are deployed in real-world applications with just a single-factor authentication. Some of the problems in single-factor authentication can be addressed with the deploying of multi-factor authentications that integrate multiple factors of authentication to enhance the security of information. Therefore, it has been increasingly important that multi-factor authentication be deployed in a massive scale to cope with the ever-growing need of information security.

As the usage of attack recognition techniques expands continuously. This research presents a plan recognition technique as attack recognition by using it in authentication. This research chooses to implement the attack recognition technique in the authentication field since there has been no previous research that has implemented the attack recognition in this field. The implementation of the attack recognition technique has long been in existence and has broadened to include the computer security domain over the past decades, especially in intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). The available researches in the field of authentication have not yet implemented the attack recognition technique into authentication schemes. Normally, this technique is implemented in language understanding and intrusion detection systems. In artificial intelligence, attack recognition is a process of analysing user action to determine their goal or result. The result will be accessed and the AI will plan the appropriate responses to any user action. However, in network security, a new set of requirements on attack recognition has been introduced.

2. Research Background

Due to the ever-increasing number of attacks that is related to authentication, there is a need to implement a newer strategy, which is called multi-factor authentication. If compared with single-factor authentication, multi-factor authentication provides a notably superior level of efficiency and accuracy. In multi-factor authentication, multiple factors are combined together to represent the authentication phase. The factors can be either knowledge, object or biometric. For biometric, it uses human features or traits such as biometric identifiers which are unique to individuals. The main advantage of biometric is the user does not need to bring or remember anything, which is quite convenient for a user. Compared to the three factors, biometric tends to be better than the other two factors. However, biometrics is also prone to a number of problems. For example and imposter may replace the biometric template with his own compromised version, which has the imposter details in order to gain access. An imposter may also steal the template for personal use.

Factor of object uses an external device or item that belongs to the user. The use of this factor, which is authentication also, has its security drawback. For example, if a user token or smart card by a legit user is stolen, an attacker may gain unauthorized access. However, unlike passwords, the user and he may know the loss of object authentication earlier or she can react appropriately to prevent any further misuse of his token or smart card.

The final factor, which is knowledge factor, uses something that is only known by the user, such as a password or a PIN (Huang, et al., 2013). In a research by O'Gorman (2003), the term password was used to include single words, phrases, and PINs (personal identification numbers) that are closely kept secrets used for authentication. An example of a strong password would be generating a random password for user authentication. However, in many real-life applications, most people create passwords based on what they remember the easiest. The likelihood of a short password will be much more susceptible to password cracking and guessing. In contrast, the use of a long and random ever-changing password makes it difficult to remember. People tend to forget these strong passwords over time.

Human authentication nowadays is carried out by multi-factor biometrics, consisting of a combination of three factors. Using this authentication, a potential user will be challenged three times before an access is granted. This will improve the overall performance of the traditional authentication scheme or single authentication scheme by checking multiple pieces of evidence of the same identity (Badrinath & Gupta., 2012).

An authentication scheme, which consists of multi-factor biometrics, refers to the use of a combination of two or more biometric modalities in a single authentication scheme. The reason of why different modalities are used is to improve the recognition rate with the use of multiple biometric features, which are independent of each other. Another reason for combining more biometrics together is the ability to match and implement the feature to multiple situation and requirement. For instance, in a home banking application, the best biometric combination would be using both voice and fingerprint. Users are able to use their fingerprint by using personal laptops or fingerprint scanners, while voice recognition can be done over the phone. Combinations of biometric modalities in an authentication scheme can also simplify user preference such as an automatic teller machine, which could use the eye,

face, fingerprint or a combination of any of these traits. Especially in demanding applications, a multi-factor biometric system is able to offer an optimum level of security and convenient for users. The use of multiple fingers for recognition is also able to provide enhance recognition capability. Authentication based on biometric alone does not ensure conclusive proof of a person's identity. The best method would be a combination of biometric with other proofs of identity such as the use of tokens or password (Bhargav-Spantzel et al., 2007).

3. Multi-Factor Authentication Scheme

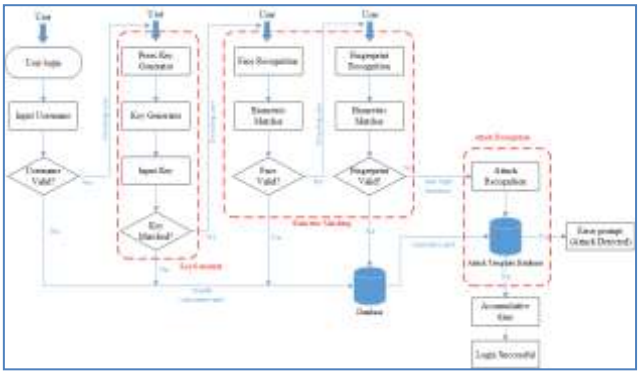

Figure 1. Flow Diagram Proposed Scheme

3.1 Key Generator

The secure key matching process is designed to be network-supported. A secure key (password) is generated upon user request. The secure key is generated based on the combination of the current date and time of when the user login process is performed. This combination will be unique as there will be no repetition of the earth date and time happening again. Compared to an earlier proposed method which uses only time factor, the number generated will not be unique as it is subject to repetition. However, by combining the time and date together, the value would be unique and cannot be repeated.

3.2 Biometric Matching

The biometric matching process refers to the process of the degree of match between two biometric traits. Usually, one biometric trait will be collected at the biometric enrolment phase and the other will be collected at the biometric verification or identification phase (authentication phase).

3.3 Attack Recognition

This research proposes a multi-factor authentication scheme and pairing it with a somewhat intelligent attack recognition technique. The method will have an attack template database which will be the main reference for the attack recognition to determine and identify any attack attempt. The attack database will have various data and signature templates of past known attacks. The attack recognition will act as an engine to analyse user input and subsequently match it with the attack template database. If a match is found, the engine will react and provide the appropriate responses to these actions. Attack recognition is important to detect and predict the future actions of the attacker to protect the system from unwanted trespassing. The integration between the multi-factor authentication scheme with the use of an attack recognition technique has never been proposed before in any previous research. But, this research is the first to integrate the attack recognition technique in authentication schemes as a new technique in authentication security. This integration was carried out to provide a good authentication scheme which able to grow and learn new attack techniques to help identify future attack and attackers.

One important component of attack recognition is the Attack Template Database. The Attack Template Database contains a description of known attacker activities and specifies the conditions which they are met. It is a form of description of the action physics for particular application domains that is applicable for building an attack in the usage domain. This database acts as a library of known attack plan cases. All the plans in the Attack Template Database must be formatted in a standard format. The Attack Template Database contains information (plans) organized into five slots which are template, vars, purpose, tasks, and orderings.
The :template slots consists of the name of the attack.
The :vars slot consists of the variables that provide the parameter for a template.
The :purpose slot defines the description of the overall purpose of the template.
The :task is a slot that consists of tasks to be performed to address the template's purpose.
The :orderings slot contains execution of actions, defined in terms of task labels.

4. Experiments

4.1 Experiments for Security

In this section, we present the security analysis that was done to test the proposed multi-factor authentication scheme. The results of several attacks done on the proposed scheme are shown. Since the proposed scheme emphasis on security, a penetration test was done via vulnerability scanning. Basically, a penetration test is an attack performed on a computer system, network or web application to find vulnerabilities that an attacker could exploit with the intention of finding security weakness and potentially gaining access to it. This research carried out a penetration test automated with software tools. The general processes involved in a system penetration test are listed below:

1. Gathering information about the target before the test (reconnaissance).
2. Identifying possible entry points (port scanning and vulnerabilities scanning) or service discovery.
3. Break-in attempt (either virtually or for real) or vulnerabilities exploitation and identification.
4. Vulnerabilities analysis.
5. Reporting the findings or evidence collection.

For security, the proposed scheme was designed to withstand attacks, which are user attacks plan (Table 1), and external attack (Table 2) that are defined in the attack recognition template.

Table1. User Attacks Plan in Attack Template Database

No.	User Attack Plan (Attack Template Database)
1.	Attempted Break in
2.	Masquerading or Successful Break in
3.	Intercepts by Unauthorized User
4.	Leakage by Illegitimate User

Table2. External Attacks in Attack Recognition

No.	External Attacks
1.	Brute Force Attack
2.	Spoofing Attack
3.	Man-in-middle Attack
4.	Replay Attack

4.2 Experiments for Accuracy

In the experiment, the FAR and FRR of the proposed scheme was compared with the FAR and FRR of the previous scheme from Raja & Perumal (2013) and Li et al (2013). Their study was chosen for comparison because the scheme has some similarities in terms of functionality and performance with the proposed scheme. Furthermore, both previous schemes also used a secure key, hence it is in-line with both experiments conducted. Even though other earlier researches were considered for comparison, these lacked the use of an algorithm, lacked experiment methods or lacked the data needed for comparison between performance measurements. The Table 3 below shows the threshold table used in the experiment (starting from strict – 99% to lenient – 84%):

Table3. Threshold for FAR and FRR

Threshold	1	2	3	4	5	6
Similarity (%)	84	87	90	93	96	99

4.3 Experiments for Efficiency

One case study was done to evaluate the efficiency of this proposed scheme. This case study consists of 15 respondents who are students from the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). The respondent's age is from 20 to 30 years old. The experiment consisted of a user case study conducted in a laboratory. The research case will follow the steps of the experimental process laid below:

A new user will need to successfully register to the system.
The user will then attempt to log in. The user will need to go through all the authentication process already mentioned in this research.
Record the time taken starting from the login attempt until the user completes the authentication process and successfully logs in. This will be taken as the result.
The result will be taken into account and be evaluated to calculate the efficiency of the scheme.
The user will then do the same enrollment and authentication process for the previous 2 schemes.
All the gathered results will be evaluated and compared with.

The proposed scheme will be compared with two (2) previous schemes from Raja & Perumal (2013) and Li et al (2013). Both of these researches were chosen because their schemes share many similarities with the proposed scheme in terms of functionality and performance. Even though other earlier researches were considered for comparison, these lacked the use of an algorithm, lacked experiment methods or lacked the data needed for comparison between performance measurements.

5. Results Analysis

5.1 Results for Security

Penetration testing is the process of discovering flaws, in systems and applications that can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration to insecure application design. The process used to look for flaws varies and is highly dependent on the particular component being tested. During the period of testing for previous scheme and proposed scheme, one (1) vulnerability in a proposed scheme, six(6) vulnerabilities for Li et al. (2013) scheme and two (2) vulnerabilities and four (4) not applicable for Raja & Perumal (2013).

Table 4. Summary of penetration test

Attack Types	Proposed Scheme	Li et al., (2013)	Raja & Perumal, (2013)
Brute Force/DOS			
TCP/IP Sequence Prediction Blind Reset Spoofing DoS	Not vulnerable	Vulnerable	Vulnerable
ICMP timestamp response	Vulnerable	Vulnerable	Vulnerable
HTTPS/SSL-Based Attack			
Self-assigned TLS/SSL certificate	Not vulnerable	Vulnerable	Not Applicable
SSL/TLS and certificate status	Not vulnerable	Vulnerable	Not Applicable
Replay Attack/Man in the Middle			
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Not vulnerable	Vulnerable	Not Applicable
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Not vulnerable	Vulnerable	Not Applicable

Based on the Table 4 above, shows the results of the penetration test for the proposed scheme, involving the developed authentication scheme based on password, fingerprint, and face. This proposed scheme was developed with the integration of security features namely attack recognition and a secure key based on the key generator technique.

From the result above, we can clearly see that the proposed scheme in this research is the most secure with only one attack vulnerability compared to the other previous schemes. Previous scheme by Li et al., (2013) and Raja & Perumal, (2013) had many vulnerabilities since they are only implementing two-factor authentication and without the attack recognition technique used by the proposed scheme.

Table 5 below shows the results of experiment of user attack plan on the proposed scheme. This experiment is conducted based on the plan in the Attack Template Database and all the respondents will follow the steps on each of user attack plan that provided in the Attack Template Database. This research does not implement any comparison with previous research because there are no previous researches applying user attack in their research. Each user were given four types of user attack in order to test the security level of the proposed scheme. The respondent's needs to follow the steps needed to trigger the user attack plan. From the

results it shows that this proposed scheme can prevent from attacks by taking following actions.

Table5. Result of User Attack Plan

User	User Attack Plan Type			
	Attempted break-in	Masquerading or successful break-in	Intercepts by unauthorized user	Leakage by illegitimate user
1	✓	✓	✓	✓
2	✓	✓	✓	✓
3	✓	✓	✓	✓
4	✓	✓	✓	✓
5	✓	✓	✓	✓
6	✓	✓	✓	✓
7	✓	✓	✓	✓
8	✓	✓	✓	✓
9	✓	✓	✓	✓
10	✓	✓	✓	✓
11	✓	✓	✓	✓
12	✓	✓	✓	✓
13	✓	✓	✓	✓
14	✓	✓	✓	✓
15	✓	✓	✓	✓
Result	Username highlighted suspicious	Username highlighted suspicious	Username highlighted suspicious	Username highlighted suspicious

5.2 Results for Accuracy

This section will show the results gathered from the experiment of accuracy. It must be mentioned that experiment was done on all 3 schemes which are the proposed scheme, Raja & Perumal (2013) and Li et al (2013).

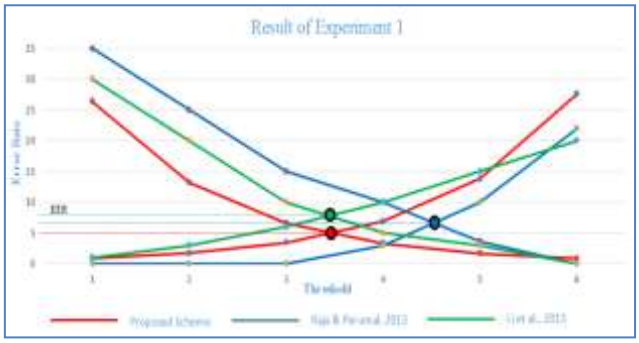

Figure 5.1 FAR, FRR and EER for Accuracy

The graphs are plotted from the FAR and FRR numbers based on FAR and FRR for each schemes. It can be seen as the threshold is increased (similarity of biometric % matching increased), the FAR decreases while the FRR increases. If the threshold decreases the FAR value will increase while the FRR decreases. This happens because when the threshold increases, the passing rate for biometric matching increases which makes it harder for users to

pass the biometric authentication. This works inversely if the threshold decreases. From the result of Figure 5.1, the EER of the proposed scheme is 5. The EER for Raja & Perumal (2013) is 7 while Li et al (2013) is 8. The accuracy of the previous scheme is 95% whereas the accuracy of the previous scheme Raja & Perumal (2013) is 93% and Li et al (2013) is 92%. From the result shown, it is clear that the proposed scheme offers higher level of accuracy. Table 5.4 below is a summary of result for experiment which is based on accuracy.

Table5.4 Summary of Result for Experiment Accuracy

Rank	Scheme	Accuracy Percentage
1	Proposed Scheme	95 %
2	Raja & Perumal, 2013	93 %
3	Li et al, 2013	92 %

In conclusion, the proposed scheme performed better in terms of accuracy with 95% of accuracy percentage when compared with the previous schemes Raja & Perumal (2013) with 93% and Li et al (2013) with 92% of accuracy percentage. The presence of the attack recognition technique in the proposed scheme proved to be the important factor in increasing the accuracy percentage. With the technique, genuine users were able to be identified correctly with minimal error. Both previous research, which lacks the attack recognition feature still scored good results but were not enough.

5.3 Results for Efficiency

Table5.5 Summary of result for Three Scheme

Rank	Scheme	Average Time (sec)
1	Proposed Scheme	15
2	Li et al, 2013	21
3	Raja & Perumal, 2013	28

In Table 5.5, the proposed scheme performed better in terms of efficiency when compared to the previous schemes Raja & Perumal (2013) and Li et al (2013). The previous scheme by Raja & Perumal, 2013 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, 2013 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.

Conclusion

This research introduces a multi-factor authentication scheme that provides increased security, by integrating the use of a secure key, user-specific fingerprint features, and facial recognition. It also adds additional layers of security, namely attack recognition and a key generator technique. This proposed research is largely motivated to the idea of improving traditional authentication by taking advantage of the capabilities of each single authentication.

These can be used to overcome some of the limitations faced by existing authentications. There have been many previous researches developing new multi-factor authentication schemes to improve security level. However, there has been no research that integrates multi-factor authentication with Artificial Intelligence in the form of attack recognition technique. Thus, this research is the first to apply a multi-factor authentication scheme with attack recognition.

Acknowledgements

Special thanks from authors for financial support (Putra Grant (GP), Project code: GP/2018/9621600) from Universiti Putra Malaysia. The principal investigator of this research project is Assoc. Prof. Dr. Nor Fazlida Mohd Sani.

References

"Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability", November 13, 2002

Al-Assam, H., Sellahewa, H., & Jassim, S. A. (2011). Accuracy and security evaluation of multi-factor biometric authentication. International Journal for Information Security Research, 1(1), 11-19.

Authentication scheme with key agreement for multimedia systems. Security and

Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security, 15(5), 529-560.Communication Networks.

Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. Computers & Security, 63, 85-116.

Deepika, C. L., & Kandaswamy, A. (2009). An algorithm for improved accuracy in unimodal biometric systems through fusion of multiple feature sets. ICGST-GVIP Journal, ISSN, 33-40.

Li, X., Niu, J., Khan, M. K., Liao, J., & Zhao, X. (2013). Robust three-factor remote user

Malik, J., Girdhar, D., Dahiya, R., & Sainarayanan, G. (2014). Reference Threshold Calculation for Biometric Authentication. International Journal of Image, Graphics and Signal Processing, 6(2), 46.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication.

Proceeding of the IEEE, 91(12), 2021-2040.

Raja, A. Y., & Perumal, S. A. (2013). Effective Method of Web Site Authentication Using

Finger Print

Sarier, N. D. (2010). Improving the accuracy and storage cost in biometric remote authentication schemes. Journal of Network and Computer Applications, 33(3), 268-274.

Sarkar, S., & Roy, A. (2013). Survey on Biometric applications for implementation of authentication in smart Governance. Researchers World, 4(4), 103.Verification. International Journal of Computer and Electrical Engineering, 5(6), 545.