International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

An Accuracy of Attack Detection using Attack Recognition Technique in Multi-Factor Authentication Scheme

Noor Aliza Mohd Ariffin, Fiza Abdul Rahim, Siti Nurulain Rum

Abstract: *One popular scheme used for authentication security is the implementation of multi-factor authentication (MFA). There have been several researches that discusses on multi-factor authentication scheme but most of these research do not entirely protect data against all types of attacks. Furthermore, most current research only focuses on improving the security part of authentication while neglecting other important parts such as the systems accuracy. Accuracy is based on how perfect is the system able to identify a genuine user or an intruder. Current multifactor authentication schemes were simply not designed to have security and accuracy as their focus. Accuracy can be measured as the success rate on tasks that requires a certain degree. For instance, the number of users who is successfully logging into the system using any technique provides a measure of accuracy. Usually, accuracy demands of users are impacted by other demands such as recall of required information, environmental, or other factors. In authentication, the accuracy factor was identified through the device pairing studies. In many cases in the authentication system requires users to enter a password or biometric traits with 100 percent accuracy for comparing it. Nevertheless, this research analyzes the level of accuracy based on the biometric accuracy of authentication. In this paper will explain the evaluation process on the accuracy level of the proposed authentication to get a highly accurate performance, which is based on FAR (false acceptance rate) and FRR (false rejection rate). Result from the experiment shows that the accuracy of proposed scheme is better than the accuracy of other previous schemes. This is even after additional security features has been added to the scheme.*

Keywords: Security; Multi-Factor Authentication; Accuracy

I. INTRODUCTION

Recent security breaches have shown that the use of single-factor authentication (SFA) mechanisms is insufficient. Security threats against poorly protected authentication mechanisms are constantly increasing [1]. Due to the problems and shortcomings of single-factor authentication mechanisms, many have turned their heads to the use of multi-factor authentication schemes (MFA). MFA will be the approach taken by industry leaders and also academic researchers.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Noor Aliza Mohd Ariffin, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia
Fiza Abdul Rahim, College of Computing and Informatics, Universiti Tenaga Nasional
Siti Nurulain Rum, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

There are three different types of elements (known as factors) that can be used for user authentication. The first would be knowledge factor, which could be a password or PIN. Object factor, the second element which could be a card with a magnetic strip or the use of a smart card. The third element which is biometric factor could be the use physical features such as face imaging, human fingerprints, or human behavioral traits for example user signature. The most common scheme for providing authenticity is the use of a password-based approach that is grouped under the knowledge factor, which has also been the most prevalent approach 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 impact users as they can easily forget their own password. This in turn will not create a healthy working environment.

As the usage of attack recognition techniques expands continuously. Basically, this research presents a plan recognition technique as attack recognition by using it in authentication. This research chooses to implement the attack recognition technique into the authentication field since there has been no previous research that has implemented the attack recognition in this field.

In general, the performance of any authentication system (e.g fingerprint, voice, facial recognition, etc) is described using several metrics. All the performance of authentication scheme is suffering from two kinds of errors such as false acceptance and false rejection of authorized users. The most common performance metrics are False Acceptance Rate (FAR) and False Rejection Rate (FRR). In addition, there are several primaries metric are particularly important to determine the accuracy of the system, that is Failure to Enrol Rate (FER) and Equal Error Rate (EER). The FER is the percentage of the users which fails to complete enrollment for an application while EER is the point at which FAR and FRR are the same. The accuracy of authentication systems is usually expressed by its equal error rate (EER). The lower this EER number is, the better the system performs. If we plot FAR and FRR on a graph, the EER is the point where the two curves intersect. The False Acceptance rate (FAR) is the probability that the system incorrectly authorizes a non-authorized user, due to incorrectly matching the biometric input with a template.

*Retrieval Number: A2629109119/2019©BEIESP
DOI: 10.35940/ijeat.A2629.109119
Journal Website: www.ijeat.org*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

The FAR is normally expressed as a percentage, following the FAR definition; this is the percentage of invalid inputs which are incorrectly accepted. While in False Rejection Rate (FRR) is the probability that the system incorrectly rejects access to an authorized user, due to failing to match the biometric input with a template. The FRR is normally expressed as a percentage, following the FRR definition; this is the percentage of valid inputs which are incorrectly rejected.

In order to consider whether the biometric features have better accuracy is based on FRR, FAR and EER. It is often to think about biometric features in terms of communications, mean that any two biometric measurements can be as the input and output of a communication channel. If the measurements are taken from the same user, they will typically be quite similar, and the FRR has become easy to measure. In contrast, if the measurements come from different users, they will typically be quite different, and the FRR has become more difficult to measure. Therefore, this proposed research implements the evaluation of proposed scheme based on measurement that are taken from the same user. According to [2], to get more accuracy and security, some systems use a combination of multiple biometric features to identify an individual. So, this proposed research uses a combination of multiple biometric features such as fingerprint and face.

First goal of this paper is to evaluate an accuracy of the proposed multi-factor biometric authentication scheme, which to determine the FRR and FAR. Two biometric traits, namely as fingerprint and face are tested in two scenarios. The different assumptions of security, such as 1) scenario A - will included with security feature and 2) scenario B - not included with security features. Security features that used in this proposed authentication scheme are secure key and plan recognition technique. Data from this evaluation would help us to understand the individual vulnerabilities of the various schemes. A second goal is to evaluate on the percentage of the accuracy between existing schemes, proposed scheme with security features and proposed scheme without security features.

II. RESEARCH BACKGROUND

An authentication system, which consists of multi-factor biometrics, refers to the use of a combination of two or more biometric modalities in a single authentication system. The reason of why different modalities are used is to improve the recognition rate with the use of multiple biometric features which are independent to 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. Uses 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 system 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 optimum level of security and also convenient to users. The use of multiple fingers for recognition is also able to provide enhance recognition capability.

Apart from security, which has become important in user identification and verification systems, accuracy is also a major concern in identification and verification systems. There are many researches out there that are struggling to improve accuracy in image processing techniques and image acquisition. The goal of having a recognition system with 0% FAR (False Acceptance Rate) and FRR (False Rejection Rate) is still far from becoming a reality despite the amount of research that has been done. Based on [3] proposed a combination of two different feature sets, which consist of statistical and extracted morphological feature. Similar biometric templates were used for both feature set which is the hand vein biometric. Their proposed research gives an accuracy result based on the speed and cost of the multimodal system. Two independent features from the same biometrics are used in this research, namely the morphological and statistical features, which are combined together. Research Sarier., (2010) focuses on remote biometrics-based verification. The research puts high importance on the range of information on every component of user biometrics separately. The result is an efficient multi-factor biometric verification system with improved accuracy and lower complexity. They conducted a comparison with an existing scheme of Bringer et al.,(2010) that achieves positive result in the reduction of computational cost and database storage.

There are many research out there who struggling to improve the accuracy in image acquisition and image processing techniques, but the amount of research which still carried out to show that recognition system with 0% FAR (False Acceptance Rate) and FRR (False Rejection Rate) is still not a reality. In this research that has produce by [3], propose a fusion of two different features sets which consist of extracted from morphological features and the other from statistical features. Both are the same biometric template which is hand vein biometric. This proposes research give an accuracy result based on the speed and cost of multimodal system. Two independent features from the same biometric are used in this research namely as morphological and statistical which combined and obtained the result an FAR of 0.3% and FRR of 0.54%. The research that has done by [5] is focus on remote biometric based verification. This research describe an efficient multi-factor biometric verification system with improve the accuracy and lower complexity by considering the range of information of every components of the user biometric separately. They make comparison with existing scheme Bringer et al is to achieve reduction of computational cost and database storage.

III. RESEARCH PROBLEM

The problem in the security paradigm is the lack of a security technique, especially in authentication systems.

A study by [10] states that the problem in security technique prevention and analysis of attacks is still a very tough topic in either the industry or academic institutions. Besides that, authentication security also has its problem.

The problem comes from a lack of design in creating a suitable encoding procedure for biometrics input signals to be converted and stored in the database. There is also a lack of matching designs to match the biometric signal received and compare it with the stored data to generate an authentication decision.

The accuracy of recognition has become the main problem in many authentication applications performed in an insecure network. The research pointed out that recognition problem has been in the limelight for some time but little to no improvement has been made since. The topic on biometric accuracy has also been highly underestimated. More needs to be done for biometric recognition to hit a satisfactory level. Furthermore, since humans are able to recognize and tell apart a person with the utmost high accuracy, the same cannot be said with biometrics where the problem is not an easy one to solve [11]. Another research states that the primary and underlying problem for accuracy performance of a biometric authentication system is caused by the limitation of the biometric identifiers. For example, the distinctive information in the geometry of a hand is less than that of a fingerprint. Thus, an increase in scale demands a need for enhanced accuracy among a larger number of targets, and therefore a higher level of matching accuracy is required [2]. Thus, with authentication systems of a large scale, it is critical to establish a matching system that reduces the volume of computations without compromising the matching accuracy. Furthermore, the matching accuracy generally drops as the matching speed increases. A method of matching at high speed while maintaining high accuracy has not yet been found [3].

IV. METHODOLOGY

A. 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 signatures templates of past known attacks. The attack recognition will act as an engine to analyze 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 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 systems 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.

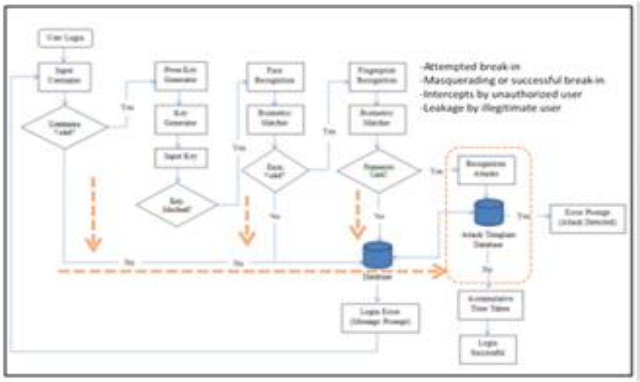
-Attempted break-in
-Masquerading or successful break-in
-Intercepts by unauthorized user
-Leakage by illegitimate user

Fig. 1 Flow Diagram Attack Recognition Technique

B. Accuracy of Proposed Scheme

This phase will firstly identify the factors to measure accuracy. Next the proposed scheme will be executed. Finally, its accuracy will be calculated and determined. In this phase, all the requirements that are needed in order to improve the accuracy of the new multi-factor authentication scheme are identified. Each different approach is adopted in the new steps of operation. To achieve this goal, this phase is divided into three steps, as follows:

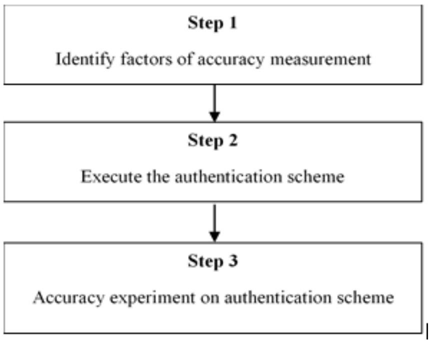
Step 1
Identify factors of accuracy measurement
Step 2
Execute the authentication scheme
Step 3
Accuracy experiment on authentication scheme

Fig. 2 Steps in Proposed Scheme

Retrieval Number: A2629109119/2019©BEIESP
DOI: 10.35940/ijeat.A2629.109119
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

To calculate and report accuracy, the output from False Rejection Rate (FRR) and False Acceptance Rate (FAR) are considered. According to [9], the industry is more towards a higher percentage of FAR and not so much on FRR. In general, it is almost impossible to get both zero FAR and FRR errors due to the fact that these classes are difficult to completely separate in the measurement space. In a biometric environment, the False Acceptance Rate (FAR) is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a template. The FAR is normally expressed as a percentage. Following the FAR definition, this is the percentage of invalid inputs, which are incorrectly accepted. Meanwhile, The False Rejection Rate (FRR) is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template. The FRR is normally expressed as a percentage, and as per the FRR definition, is the percentage of valid inputs, which are incorrectly rejected.

The multi-factor authentication scheme is fully executed together with its connection to the database. The system environment of the scheme is intended for installation on the server side (web-based) and linked back to the database, which is located in a remote location. However, for this analysis, the application and database will be located in the same workstation.

General, the performance of any biometric authentication system is measure using several metrics. The most common performance metric for accuracy is the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The False Acceptance Rate (FAR) is the probability that the system incorrectly authorizes a non-authorized user, due to incorrectly matching the biometric input with a template. The FAR is normally expressed as a percentage. Following the FAR definition, this is the percentage of invalid inputs, which are incorrectly accepted. On the other hand, the False Rejection Rate (FRR) is the probability that the system incorrectly rejects access to an authorized user. It is due to the system failure to correctly match the biometric input with a template. The FRR is normally expressed as a percentage. Following the FRR definition, this is the percentage of valid inputs, which are incorrectly rejected. An experiment on accuracy will be conducted on the proposed authentication scheme using FAR and FRR. The percentage result of both FAR and FRR will reflect the accuracy of the proposed scheme. FAR and FRR will also be done on current available schemes. The result of all experiment will be compared and valued.

V. EXPERIMENTS FOR ACCURACY

The literature on biometric authentication systems suggests that high FAR and FRR values pose a significant problem. However, in some cases it is sometimes impossible to reduce both FAR and FRR to a much lower rate. If the system requires a very close match, FAR will be low in value, but FRR will still be high in value, and vice versa. In order to accomplish this goal, this research conducted two experiments.

The main goal of this chapter is to evaluate the accuracy of the proposed multi-factor biometric authentication scheme, and to determine the FRR and FAR. 2 types of experiment were done which is the accuracy of the scheme with the use of a secure key (key generator) and accuracy of the scheme without a security key. On both experiments, the proposed scheme were compared with 2 previous schemes which are (Raja & Perumal, 2013) and (Li et al., 2013). Refer to the Figure 3 for the experiment on accuracy.

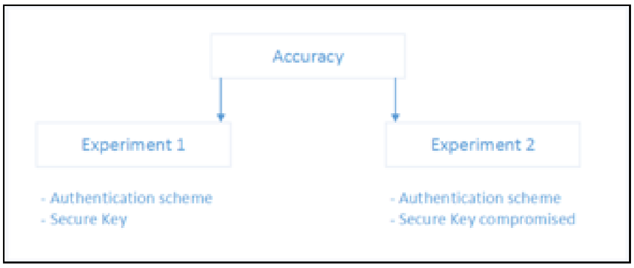

Fig. 3 Experiment on Accuracy

In summary, experiment 1 accuracy will be based on the fully function techniques from all the schemes. Experiment 2 will omit the function of secure key to imitate the loss of a secure key or in other words the key is compromised.

In the first 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 that of 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.

Usually, the FAR is determined by conducting an experiment with user A using his own fingerprint and face to try and authenticate as user B, and vice versa. It is certainly important that a biometric authentication scheme rejects such attempts. For FRR, user A and B will try to authenticate as themselves. Since they are using their own credentials they should be allowed to authenticate. This research therefore uses the independent performance measurement of EER which is the point where FAR and FRR intersect if they are put in graphical form. The lower the EER, the more accurate the system is considered to be. Figure 4 shows the user process which was run for both experiment 1 and 2:

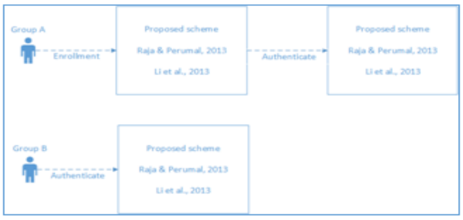

Fig. 4 User Process for Both Experiments

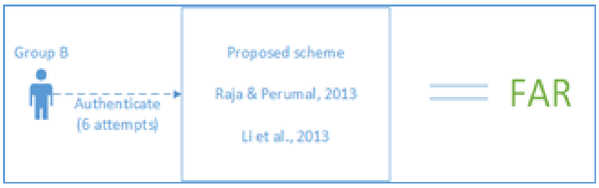

Fig. 5 FAR Process

For the calculation of FAR, Group B respondents which does not have any saved credentials on the system are required to log in to all 3 schemes proposed scheme, Raja & Perumal (2013) and Li et al (2013). In a perfect scenario, none of the respondents in group B should be able to log in. But in the experiment done, each user authentication attempt and result were taken. Any respondents which were able to successfully login will considered as system breach and contribute to the calculation of FAR.

In contrast, FRR will require group a respondents which are supposed to be legitimate users to authenticate to all 3 schemes proposed scheme, Raja & Perumal (2013) and Li et al (2013). Figure 6. below shows the action done by group A respondents.

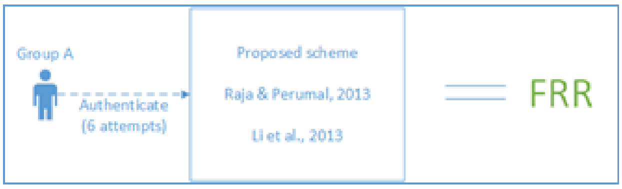

Fig. 6 FRR Process

Group A respondents having their details already registered in the systems should be able to successfully log in. In the experiment, any respondent which were denied access to the system are considered false rejection and again contribute to the calculation of FRR. Figure 7 is the summary of all the experiments.

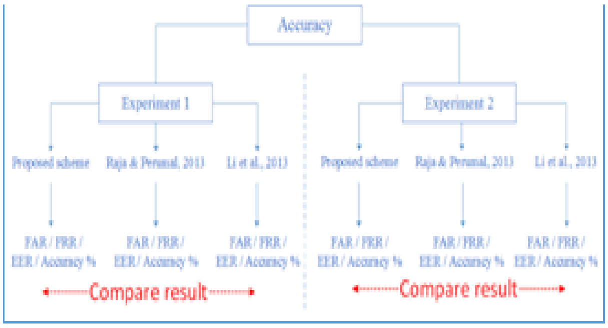
Accuracy
Experiment 1
Experiment 2
Proposed scheme
Raja & Perumal, 2013
Li et al., 2013
Proposed scheme
Raja & Perumal, 2013
Li et al., 2013
FAR / FRR / EER / Accuracy %
FAR / FRR / EER / Accuracy %
FAR / FRR / EER / Accuracy %
FAR / FRR / EER / Accuracy %
FAR / FRR / EER / Accuracy %
FAR / FRR / EER / Accuracy %
Compare result
Compare result

Fig. 7 Summary for Both Experiments

To obtain the EER value, the FAR and FRR must be plotted in a graph. EER is the point where the two curves of FAR and FRR intersect. Another factor which determines the EER and accuracy percentage is the threshold. For this experiment, the threshold is the similarity between the received biometric information from user and the biometric information stored in the database. Table I shows the threshold table used in the experiment (starting from strict – 99% to lenient – 84%):

Table. 1 Threshold for FAR and FRR

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

VI. RESULTS FOR ACCURACY

A. Results of the First Experiment

This section will show the results gathered from the first experiment. It must be mentioned that the first experiment was done on all 3 schemes which are the proposed scheme, Raja & Perumal (2013) and Li et al (2013). The first experiment uses all the security factors on all 3 schemes. The results were taken from the experiment done by all 30 respondents in group A and B. Figure 8 shows FAR, FRR and EER for all 3 schemes in experiment 1.

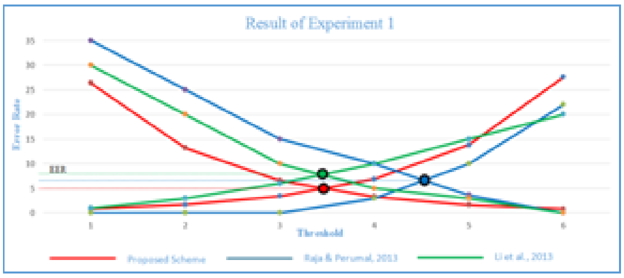

Fig. 8 FAR, FRR and EER for Experiment 1

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. Table II is a summary of result for experiment 1 which is based on accuracy.

Table. 2 Summary of Result for Experiment 1

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.

B. Results of the Second Experiment

The second experiment was done on all 3 schemes which are the proposed scheme, Raja & Perumal (2013) and Li et al (2013). On the second experiment, the security factor of secure key (key generator) was omitted from all 3 schemes to simulate an authentication process which is unsecured because of a compromised key. The results were taken from the experiment done by all 30 respondents in group A and B. Figure 9 shows FAR, FRR and EER for both schemes in this experiment.

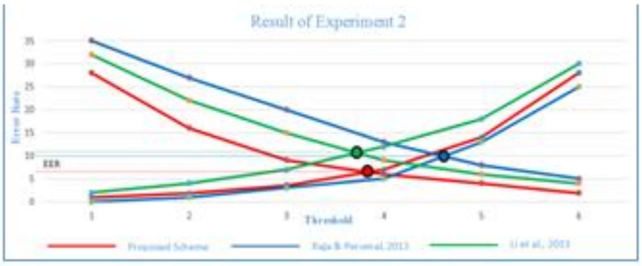

Fig. 9 FAR, FRR and EER for Experiment 2

Similar to experiment 1, the FAR and FRR result is highly dependent on the threshold value. If the threshold increases, the FAR value will decrease while the FRR value increases. When the threshold increases, imposters or attackers are denied access (contribute FAR) while genuine users are also sometimes denied access (contribute to FRR). However when the threshold decreases, imposters or attackers are sometimes able to login to the system (contribute to FAR) while legitimate users are also allowed access (contribute to FRR). This is due to the leniency of the biometric matching percentage. Table III is a summary of result for experiment 2 which is based on accuracy.

Table. 3 Summary of Result for Experiment 2

Rank	Scheme	Accuracy Percentage
1	Proposed Scheme	93 %
2	Raja & Perumal, 2013	90 %
3	Li et al, 2013	89 %

VII. CONCLUSIONS

We have investigated the accuracy of multi-factor authentication schemes for two commonly used biometric traits namely fingerprint and face. We have demonstrated that in the case of insecure scheme, the accuracy of proposed scheme is drops. Furthermore, this paper also shows experiments conducted on proposed scheme with enhanced the accuracy performance. Here, we note that, the experiment results showed that both proposed scheme secure and insecure are more accurate based on FAR, EER. It can be clearly noticed that apart from our results, the better authentication accuracy was reported when the schemes to be secure with achieving low FAR. The schemes that have less security will get high FAR and accuracy Percentage. These results highlight a serious security implication for insecure schemes.

REFERENCES

1. Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. Pattern Recognition, 48(2), 458-472.
2. Sarkar, S., & Roy, A. (2013). Survey on Biometric applications for implementation of authentication in smart Governance. Researchers World, 4(4), 103.
3. 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.
4. 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.
5. 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.
6. "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability", November 13, 2002
7. 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.
8. 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.
9. Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. Computers & Security, 63, 85-116.
10. Li, X., Niu, J., Khan, M. K., Liao, J., & Zhao, X. (2013). Robust three factor remote user authentication scheme with key agreement for multimedia systems. Security and Communication Networks.
11. Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (2013). Secure biometrics: concepts, authentication architectures, and challenges. Signal Processing Magazine, IEEE, 30(5), 51-64.