Efficiency of Secured Novel Multi-Factor Authentication Scheme with Biometric Technology

Noor Afiza Mohd Ariffin, Nor Fazlida Mohd Sani, Zurina Mohd. Hanapi, Ramlan Mahmod

Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), 43400 Serdang, Selangor, Malaysia.

ABSTRACT

Providing authentication mechanisms over network is one of the paramount for the development to delivery application. This need is particularly strongly authentication to ensure the security will be delivered into the applications. However, this turns out to be challenging issues such as security and efficiency. There are several schemes have been proposed regarding the multi-factor authentication from time to time. However, the previous schemes are still vulnerable to various attacks such as brute force attack and dictionary attack and not achieving efficiency in term of execution time performance. In this paper, an efficient authentication scheme is proposed which is suitable for every network layer. It proposed plan recognition technique which can detect, identify and help to authenticate the users and it can effectively defend all known attack such as brute force attack and dictionary attack also provide low execution time performance.

INTRODUCTION

The rapid progress of network facilities would bring a more computers connecting together to exchange a great information and share the system resources. So, the security becomes an important issue for computer networks. Basically, there are two basic requirements for network security such as secrecy and authentication. Secrecy protects sensitive data against eavesdropping and modification. Whereas authentication prevents forgery and unauthorized network access. Traditionally, identity authentication in computer systems is based on key, PIN or password. The most common scheme to provide authenticity is the use of passwords. Password authentication has been used for a long time and mainly because it is easy to implement, easy to use and cheap. But, all the things like a key or card is tending to get stolen or lost and the password also often forgotten. Security constraints should be given at the highest level in authentication based network system. This is a basic principle for build-up secure system and it reflects the fact that at the authentication level should know what needs should be allow or restrict based on the needs of the system.

In other hand, biometrics technology provides a strong user authentication solution. In technological era development today, in every aspect of human life are replacing with machine. So the security concern is need and increase to automate the different surveillance techniques and authentication checking of the users. To achieve more secure identification in authentication, it should combine with something that really characterizes the given person. Biometrics offers automated schemes of identity verification on the principle of measurable physiological or behavioral such as fingerprint or voice sample. The characteristics are measurable and must be unique. Although biometric techniques are more secure in authentication process compare to another technique but they still open to vulnerable attack such as spoofing attack because mostly authentication are deployed in real world applications with a single factor authentication. Some of this problem in single authentication such as security in privacy information may overcome with deploying multi-factor authentications scheme that integrates of multiple factors of authentication.

This purpose of this research is to help the users to feel secure when using any authentication application. The highest priority in authentication that proposes by this research is efficiency and security when a user’s accessing sensitive information.

Corresponding Author: Nor Fazlida Mohd Sani, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), 434000 Serdang, Selangor, Malaysia.
E-mail: fazlida@upm.edu.my
Related work:

A. Security and Authentication:

In the computing world, the security takes an increasingly predominant role. This is a challenge to discover the vulnerabilities and customer also expect security to be delivered in the system. The most important securities primitive is an authentication. Basically, authentication is the process of verifying and determining the people who are requested to use a resource who is declared to be. Generally, the authentication can be categorized into three categories: 1) knowledge-based such as using a password or PIN, 2) object-based which based on something possesses such as smart card and 3) biometric-based which relies on some personal characteristics of a person such as iris, fingerprint, facial and voice.

For decades, single-factor authentication (SFA) has been used for many authentication applications. Single-factor authentication (SFA) is a process for securing access to a given system, such as a network or application which identifies the party requesting access through only one category of credentials Margaret,Rouse (2011). The password has been the standard means for user authentication on computers. However, as users are required to remember more, longer, and changing passwords, it is evident that a more convenient and secure solution to user authentication is necessary, O'Gorman, L. (2011).

One of the main troubles with passwords is that most users either don’t understand how to make strong and memorable passwords or underestimate the need for security, Margaret and Rouse (2011). The common techniques of single user authentication which involve the password can be easily illicitly acquired by direct covert observation, O'Gorman, L., (2011). Once an intruder acquires the user ID and the password, the intruder has total access to the user’s resources. In addition, there is no way to positively link the usage of the system to the actual user, that is, there is no protection through brute force and dictionary attack. For example, when a user ID and password is entered by intruder, there is no way for the system to know who the actual user is. A similar situation arises when a transaction involving a credit card number is conducted on the Web. Even though the data are sent over the Web using secure encryption methods, current systems are not capable of assuring that the transaction was initiated by the rightful owner of the credit card. In the modern distributed systems environment, the traditional authentication policy based on a simple combination of user ID and password has become inadequate, O'Gorman, L. (2011).

Ross and Jain (2014) stated that the unimodal biometric systems suffers from a variety of problems like noisy sensor data, non-universality, restricted degree of freedom, intra-class variations, spoof attacks and unacceptable error rates. Some of these problems of single trait biometric systems can be overcome by designing multimodal biometric systems which provides multiple evidence of the same feature, Kaur, R., and Tulwar, M. (2013). According to Ratha et al., (2001), the biometrics-based authentication offers several advantages than other authentication schemes. But it also has some limitation, for instance if the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication. Another limitation of biometric single authentication such as the tip of the finger is a small area from which to take measurements, and ridge patterns can be affected by cuts, dirt, or even wear and tear.

Acquiring high-quality images of distinctive fingerprint ridges and minutiae is complicated task. People with no or few minutia points (surgeons as they often wash their hands with strong detergents, builders, and people with special skin conditions) cannot enroll or use the system. The number of minutia points can be a limiting factor for security of the algorithm. Results can also be confused caused by false minutia points (areas of obfuscation that appear due to low-quality enrollment, imaging, or fingerprint ridge detail).

B. Multi-Factor Authentication (MFA):

The increasing number of authenticated applications and the constant growing of attacks seem to call for multi-factor authentication technologies. Multi-factor authentications are considered stronger authentication as they combine several of the following authentication factors: 1) knowledge-based, that is something only known by the user, like a password or a PIN. 2) object-based, that is something the user possesses, like a physical token. 3) identity-based, that is a user's feature, i.e. biometrics, which relies on the uniqueness of a physical characteristic of a person such as fingerprints, facial features, iris, and voice, Huang, Y., et al. (2013). Research from N. Ratha et al. (1995) proposed a new scheme for efficient feature extraction from fingerprint images based on ridge flow orientations. The performance evaluation has been described based on execution time with the comparison the detected features to the ground truth and the proposed scheme have been tested on 100 fingerprint images.

The research Sadi et al. (2011) implement an simulation of fingerprint verification using three approaches- biometric technique, Genetic algorithm and Back propagation neural network. The performance of the three approaches was assessed in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR) and execution time. The proposed authentication scheme by Gnanaraj et al. (2013) has provided an enhanced security with an optimal overall time taken for the operation. The proposed scheme utilizes the biometric data embedded in a smart card along with the ID and password of the user. This research also will compare...
the time efficient performance with the existing Secure Socket Layer based authentication scheme and attacks which the proposed scheme is able to withstand.

A new technique proposed by the Mathew and Thomas (2013), that uses cued click point graphical password method along with the one-time session key is proposed. The goal is to propose a new authentication mechanism using graphical password to achieve higher security and efficiency levels in term of time performance. The result of the system testing is evaluated and it reveals that the proposed system ensures security and efficiency to a great extent. In order to evaluate the security and efficiency of the system, the simulation is conducted using a group of 15 students in the age between 20 and 30 and questionnaires were prepared. This simulation measure a login time start from the users takes for registration until first time login. The result shows that the users take more time for registration since they were new to the system. The login time is reduced in each time when they login to the system. Whereas the successive login to the system will reduce the login time of each user. This result reveals that the users feel convenient in using the system.

A. Rattani et al. (2013), proposed a multimodal biometric system using Finger print and Face. They use Scale Invariant Features Transform (SIFT), Fingerprint Verification based on Minutiae matching Technique and Feature Level Fusion for the recognition. Research from F. Besbes et al. (2008) proposed a multimodal biometric system using Fingerprint and Iris features. This approach was based on two recognition modalities and every part provided its own decision No experimental results have been reported for recognition performance.

C. Comparison and Discussion:

According to the research from N. Ratha et al. (1995) proposed a new scheme for feature extraction fingerprint images. This proposed method not efficiency because it still has high execution time. So, it cannot be acceptable for commercial use because it have high execution time. Research from Jain et al. (1997), describes the design and implementation of a prototype automatic identity-authentication system that uses fingerprints to authenticate the identity of an individual. They have developed an improved minutiae-extraction algorithm that is faster in term of response-time and more accurate than other research. Tan and Bhanu (2006) applied GA for fingerprint matching. They included biometric properties of fingerprints in their matching. This researchers scheme claims that their scheme has provide an efficient authentication, however, their scheme is still have a high execution time. Recently, Lin-Lai (2004) proposed 'a flexible biometrics remote user authentication scheme,’ which is based on El Gamal's cryptosystem and fingerprint verification, and does not need to maintain verification tables on the server. They claimed that their scheme is secured from attacks and suitable for high security applications; however, their scheme is vulnerable and can easily be cryptanalyzed. Research from Bhargav - Spantzel et al. (2006), propose a two-phase authentication mechanism for federated identity management systems. The first phase consists of a two-factor biometric authentication based on zero knowledge proofs. They research has several security and privacy advantages in authentication. Research from Lee and Liu et al. (2009) has change the passwords in local without notifying the server, thus it can decrease the communication overheads and some possible attacks between two communications parties over an insecure network. Based on the research from Hwang and Li (2000), not efficient in terms of communication and computation cost. It is because they use a password 1024 bits that is very hard for user to memory. Furthermore, the security of Hwang and Li’s scheme is based on the difficulty of the discrete logarithm problem. Once the discrete logarithm problem is solved, then their scheme will become insecure.

Table 1: Capability of Existing Research

<table>
<thead>
<tr>
<th>Authentication Scheme</th>
<th>Security Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Efficiency</td>
</tr>
<tr>
<td>1. N. Ratha et al., 1995</td>
<td>×</td>
</tr>
<tr>
<td>2. Jain , et al., 1997</td>
<td>×</td>
</tr>
<tr>
<td>3. Tan and Bhanu, 2006</td>
<td>×</td>
</tr>
<tr>
<td>5. Lin-Lai, 2004</td>
<td>×</td>
</tr>
<tr>
<td>6. Bhargav - Spantzel et al, 2006</td>
<td>✓</td>
</tr>
<tr>
<td>7. Lee &amp; Liu et al, 2009</td>
<td>×</td>
</tr>
<tr>
<td>8. Hwang and Li, 2000</td>
<td>×</td>
</tr>
<tr>
<td>9. Proposed Scheme</td>
<td>✓</td>
</tr>
</tbody>
</table>

MATERIALS AND METHODS

This research contains three phases of methodology as follows:

Identify and evaluate performance efficiency of novel authentication
Execute a novel authentication scheme
The novel authentication scheme must to execute and connected the scheme with plan formalism by using connection of database in order to evaluate the performance of novel authentication scheme.

**Analyzing the result:**

This step is done as manually to identify the pattern of result that will consider in this research. For instance, the result that produces in this research in term of execution time. This is the time calculated as the time taken to take the input, compare with database and produce the results. This is measured in seconds.

**Comparative Analysis:**

In this step, the result that had been obtained will be compared with previous research as manually to ensure the proposed scheme is more efficiency in term of time performance.

---

**RESULTS AND DISCUSSION**

This research present experimental result that have already undertaken concerning the effectiveness of proposed scheme. To test the effectiveness of our scheme, this research has conducted an experiment to validate the use of proposed scheme. One of the objectives of this research is to measure the effectiveness of scheme based on the time that takes to authenticate users. Our experiment consisted of a user study conducted in a laboratory. Each user will follow the steps in experiment 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 results from this research will be compared with previous research.

In the experiment, the proposed scheme and a previous scheme uses a different technique in authentication; the propose scheme use a plan recognition technique while the previous scheme uses several technique such as biometric technique, Genetic algorithm and Back propagation neural network. The time taken in this experiment is based on the time taken to take the input, compare with database and produce the results in unit second (sec). Figure below shows the graphs the result from proposed scheme between previous scheme. It shows the execution time performance proposed scheme is faster than the execution time performance for previous scheme. Although this proposed scheme use more than one factor in authentication, its still can provide a low execution time performance.
Conclusion And Future Work:

This research propose a novel multi-factor authentication which integrate the three factor such as password, fingerprint and face which never been use in any previous research. It proposes plan recognition technique which can detect, identify and help to authenticate the users in network based with low execution time performance which are not supported by the previous scheme. In addition, this paper performed performance comparison with some existing schemes to proof that this research has low execution time performance compare to others. This proposed scheme also can resist popular attacks such as brute force attack and dictionary attack.

REFERENCES


Praveena, T.L., V. Ramachandran and C.H. Rupa, Attribute based MultiFa Authentication for Cloud Applications


Sani, N.F.M., N.A.M. Ariffin and R. Atan, 2013. DESIGN OF OBJECT-ORIENTED DEBUGGER MODEL BY USING UNIFIED MODELING