Improving Information Security in E-Banking by Using Biometric Fingerprint

A CASE OF MAJOR BANK IN MALAYSIA

Mahmoud Mohammed Mahmoud Musleh
Department of Information Systems
International Islamic University Malaysia, IIUM
Kuala Lumpur, Malaysia
mahmd.musleh@gmail.com

Ismail Idrissa Ba
Department of Information Systems
International Islamic University Malaysia, IIUM
Kuala Lumpur, Malaysia
ba1ismaila@yahoo.fr

Karama M.A. Nofal
Department of Information Systems
International Islamic University Malaysia, IIUM
Kuala Lumpur, Malaysia
karama.nofal@gmail.com

Jamaludin Ibrahim
Department of Information Systems
International Islamic University Malaysia, IIUM
Kuala Lumpur, Malaysia
jamaludinibrahim@kict.iium.edu.my

***Abstract*— In this paper biometric fingerprint technology will define and discuss as new best approach identification and authentication customers for online internet banking, and how biometric fingerprint will improve the internet banking protect its assets. Background will be produced to present how authentication and identification have developed and improved through the applications successful that have implemented biometric technology to protect its asset; then a case of major bank in Malaysia will be taken as a case study. By answering the question, why does biometric fingerprint need to come forefront as a great method of authentication in online banking environment? The findings have found that there are reasons and factors for higher security as a near perfect and biometric fingerprint authentication will be indicated to be the solution to answer this call.**

Keywords- Biometric Fingerprint; E-banking; Information Security; Online Banking; Biometric Technology

I. INTRODUCTION

Millions of dollars are being invested in the developed of e-banking systems worldwide, and it is of paramount importance that these systems are fully utilized by potential customers. However, there remains reluctance by consumers to accept e-banking because of the perceived risk security financial and time. Therefore, banks need to better understand their customers and respond to developments in internet technology in a way that incorporates their customers' requirements and addresses their concerns [16].

There are three major types of authentication commonly used; the first type is something that you know such as a password, PIN or a piece of personal information. Secondly, it is something that you have such as a smart card or token. The last type is something that you are such as a biometric [10]. On the other hand, many organizations are using the internet as a new distribution channel to provide their customers a good service such as internet banking [14]. This channel needs to be secure and trusted not only to protect the customer information from fishing or hacking, but also provide data integrity; and to ensure providing the services in a safety way. Therefore, Information security has become a major concern for banks to conserve their customers' assets. In addition, everyday there are updates of security to face the challenges that have faced internet banking; in parallel, there are intruders who think every moment to attack others. This paper will focus on biometric fingerprint technology as a solution to deter the threats that concerns e-banking security as much as possible.

A. Background of Study

Issues with biometric device include accuracy and failure. Some researchers mentioned that biometric still have negative impact denying access to unauthorized user. What happen if the user is wearing a bandage on the finger of authentication? For this scenario some device provide password. One of the issues regarding biometric is cost effective, in today organization user work in the office, at home, and in hotel, airport, and internet café. If you decide to purchase biometric device for all employees, how many device will you buy? [2]. While others have seen a biometric fingerprint is a powerful way of deciding who can gain access to our most valuable system in this modern world; despite biometric fingerprint are successfully adopted in areas such as Automatic Teller Machine (ATM) [4, 15]; however, there is a lack of implementation to online banking environment [17].

According to online banking of two major banks in Malaysia, customers used username and password to access their accounts. However, the difference is that one uses TAC number to authenticate when the customer needs to make transaction, and another thing the customer has to answer questions that he knew the words exactly when customer subscribed in the internet banking and he put his own answer.

As a result, biometric fingerprint as a near perfect security is still in its infancy for most major banks in Malaysia. Those did not take a risk in order to achieve biometric solution to enhance their security systems. Some opponents argue that password only authenticate a password but not the user. Password can be forgotten and forged by the hackers. Password does not provide a non-repudiation security service which means to ensure that transferred message has been sent and received by the parties claiming to have sent and received the message and also password is very vulnerable [3]. Biometric method will basically authenticate the person and internet banking that must have a non-repudiation security service to ensure that customer cannot later deny his transaction. Some security expert argue that biometric is the only true user authentication because of it physical authentication [2]. As some people will see, biometric will not be the best choice for every one [5]. On the other hand, biometric technology appeals to many banking organizations as a near perfect solution to such security threats [17]. Therefore, the biometric fingerprint technology is the best method to protect and secure online banking assets. The banks should adopt biometric fingerprint technology as a near perfect solution to such security threats of internet banking in particular for major bank in Malaysia.

B. Scope of Study

This study will focus on factors that influence the bank to be ready to use biometric fingerprint to authenticate the user when make transaction on internet banking. Existing literatures will be used to design the study. Although there are many researches talk about biometric technology available in various literatures, but this study will focus on only the biometric fingerprint to investigate whether the major bank in Malaysia ready to use biometric fingerprint in internet banking. Qualitative will be used to carry this paper, sample will be chosen, and afterwards gathering information and analysis will be performed.

C. The Significance

The paradigm shift from something that the users know to something that the users are; online banking requires the development and implementation of trustworthy security procedure [7]. Therefore, the newly emerged service such as fingerprint biometric to use it in the internet banking for authentication and identification and rapidly increasing penetration rates of internet banking to be as near perfect security are the motivators of this study [13].

- Biometric fingerprint considers as a new technology in online banking environment which means it needs a lot of efforts and resources to be used.
- The biometric fingerprint has become a significant phenomenon in recent times, it has various advantages and benefits in both organization and customer.

II. LITERATURE REVIEW

A. An overview of Information Security

With the rapid growth of Information and Communication Technology (ICT), information security becomes more pervasive in everyday lives while there are many channels and methods to attack of websites with this great development of information security. One of the threats to web authentication is phishing, where a phishing attack is a type of social engineering attack, designing users' authentication credentials by spoofing the login page of a trusted web site [9]. However, some banks in Malaysia use TAC number by sending it to customer's mobile to authenticate the user when he make transaction and others use the questions that the customer has already known his own answer when he subscribed in internet banking.

Some opponents argue that the information which the person knew such as a password only authenticate a password but not the user and can be forgotten and forged. The information such as the question that supposed the customers knew can be forgotten and forged by the hackers [2]. Furthermore, Password does not provide a non-repudiation security service and the passwords are easily broken with the programs that available on the internet that help to break the password and may be people will choose easily remembered and easily gassed password such as name of their relative, date of birth or phone number [12, 3].

B. Online Banking Security with Biometric

Online banking demands the development and implementation of trustworthy security procedure [7]. This requirement needs to design effective method that works efficiently via which users or customers can be verified and authenticated in a remote environment.

The biometric fingerprint has become an important phenomenon in recent times, it has various advantages and benefits in both organization and customer [13]. However, it is yet to be adopted by major bank in Malaysia.

Many studies have been conducted on biometric fingerprint technology, and many researchers have discussed the influence that biometric technology as a perfect solution for many purposes [4, 5, 13, & 17]. In contrast, there is still a lack of research on the factors or the ability of banks to be ready to use biometric fingerprint in internet banking to authenticate the user.

C. Definitions of Terms Used

1) Information Security in Business

In business information security helps managers to govern, monitor and secure the information from malware changes and removals or unauthorized access. The main aims of Information security in business is to protect the confidentiality from a competitor or media and integrity that is to ensure that

the information is not changed or modified as well to ensure the availability of the information when needed or in an event of a disaster [12]. Many businesses are merely depending on information deposited in computers; personal information, and details that may all be warehoused on a database. Without this information, it would often be very hard for a business to function. Information security systems need to be implemented to protect this asset [2].

Nowadays, there are many types of threats available on the internet that need to be enforced to ensure business goals. Based on Proctor, 2002 organizations and their information system and network are faced with security threat from wide range of sources including computer fraud, espionage, sabotage, and vandalism [18]. Cause of damage such as code, computer hacker and denial for services attach have become more common and increasingly spreading in the World Wide Web.

2) Security Policy

A policy is a document that summarizes rules that must be abided by the organization. Security policy is the backbone of the security architecture without a policy you cannot protect your information [2]. In addition, policies allow the organization to reduce cost and eliminate accountability. Written policy works as the means of communicating company guidelines to the customer [11]. Furthermore, policy defines how security should be implemented, this comprise proper configuration. Thus policy provides the rules that govern how system should be configured and how customers of an organization should act in normal circumstance and react during unusual situation. Some examples recommended for biometric Policy; do not share your fingerprint device with any person, any obvious act of fraud or guessing the fingerprint the services will be terminated report to the bank immediately when the device is stolen.

3) Biometric Fingerprint

The term biometrics is used to describe physical dimensions and/or behaviour characteristics which are essential and unique to the human being; and it can be utilized to verify the identity of a person. These characteristics include fingerprint, hand geometry, facial characteristics, iris, retina, personal scent and DNA, while behaviour features include handwriting, keystroke, voice and gait. Physiological characteristics can be measured and recognized [8]. Biometric fingerprint technology is considered one of the most secure and convenient authentication tool. It cannot be stolen, borrowed, or forgotten, and forged [10].

III. The Difficulties and Challenges the Project Faced

Getting information from the banks is very challenging because of the sensitivity asset; in addition, the bank policy stated that it is illegal to reveal the customers' information and their strategy plan. Furthermore, the bank delayed to respond our request to meet the human resource manager. Since there is a high competition among the banks, so every bank wants to keep their strategies from the researchers and press. Asset protection is the biggest challenge in information security systems of the banks. They have sensitive information such as customers' information and their credit card details, which need to be secured. Therefore, protecting information against leakage has become more complex and difficult when an opponent who is authorized to view the data or information about the processes of the security system [1].

Based on Harris & Spence, 2002 banks are increasingly threatened by the leakage of sensitive information which can be available to impostors or competitors. Furthermore, Banks want to ensure that information assets such as the security system, trade secrets, software code, designs, architectures, and algorithms are not leaked and abused [6]. Also, they want protection against leakage of internal confidential information, which can damage the customers' trust to the company brand.

According to these reasons the major bank in Malaysia rejected to give us any information about their e-banking security system; to avoid leakage of information which can compromise their security system and affect their competitiveness of protecting the confidential information of their customers.

IV. Proposed E-banking security system processes

A. Authentication processes to access the account

The diagram shows that the authentication process consists of two stages. First of all, the user needs to verify his/her username and password, if the username and the password are accepted; the browser will direct the user to the second stage of authentication but if the username and the password are not accepted the browser will ask the user to reinsert valid username and password.

Secondly, this stage is the most significant one which is the authentication stage by using the biometric fingerprint technology. The user needs to verify his/her fingerprint by using fingerprint reader which is connected to his/her own personal computer (Figure 1). The fingerprint server will match the user fingerprint with the bank's fingerprints database; if it is accepted the browser will direct the user to access his/her accounts.

These two stages of authentication protect the customer information from unauthorized reading that means confidentiality of the customer which is very important from the customer's perspective because it saves him/her from failing under the threat of the malicious people.

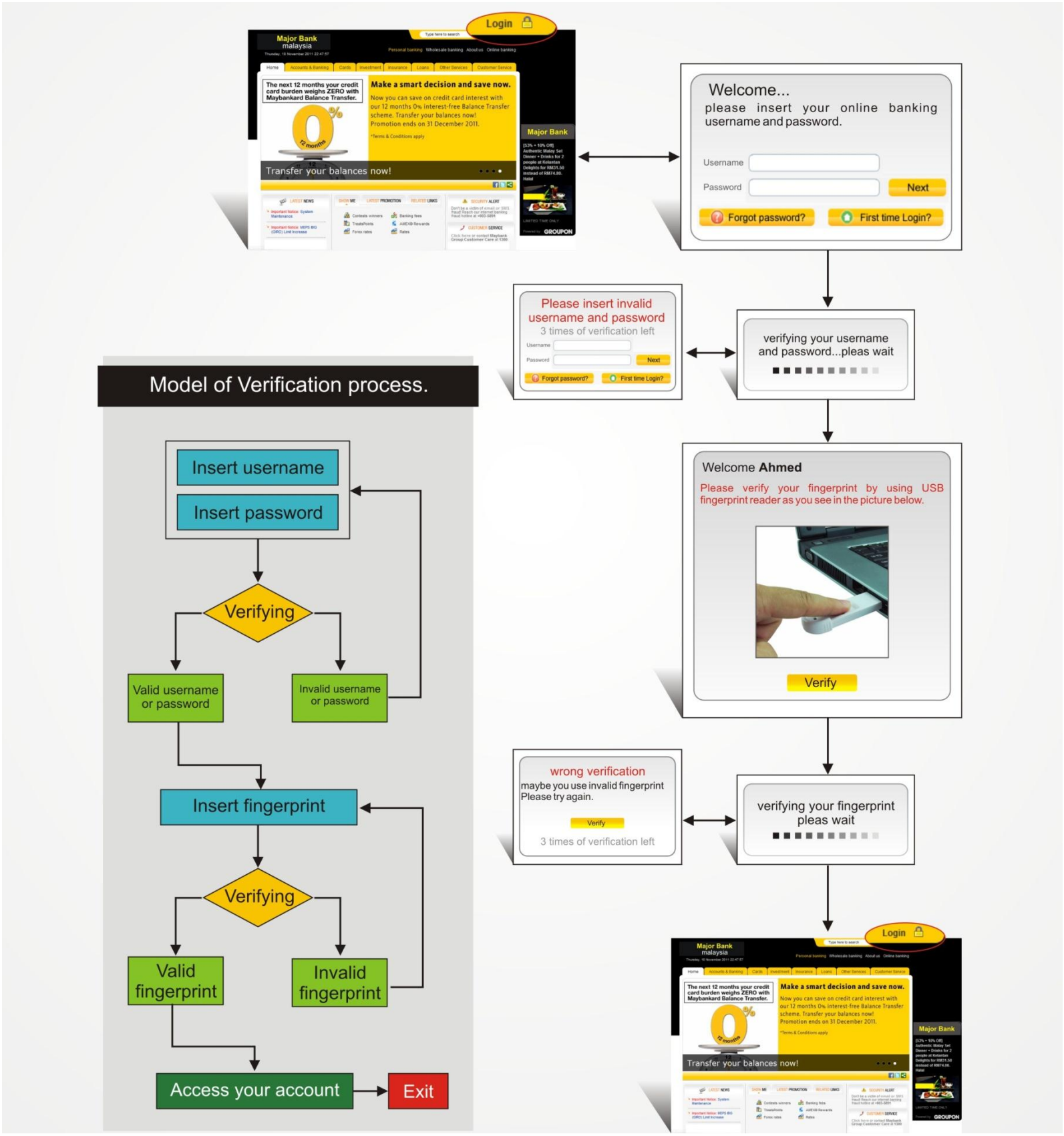

Figure 1. Authentication processes to access the account

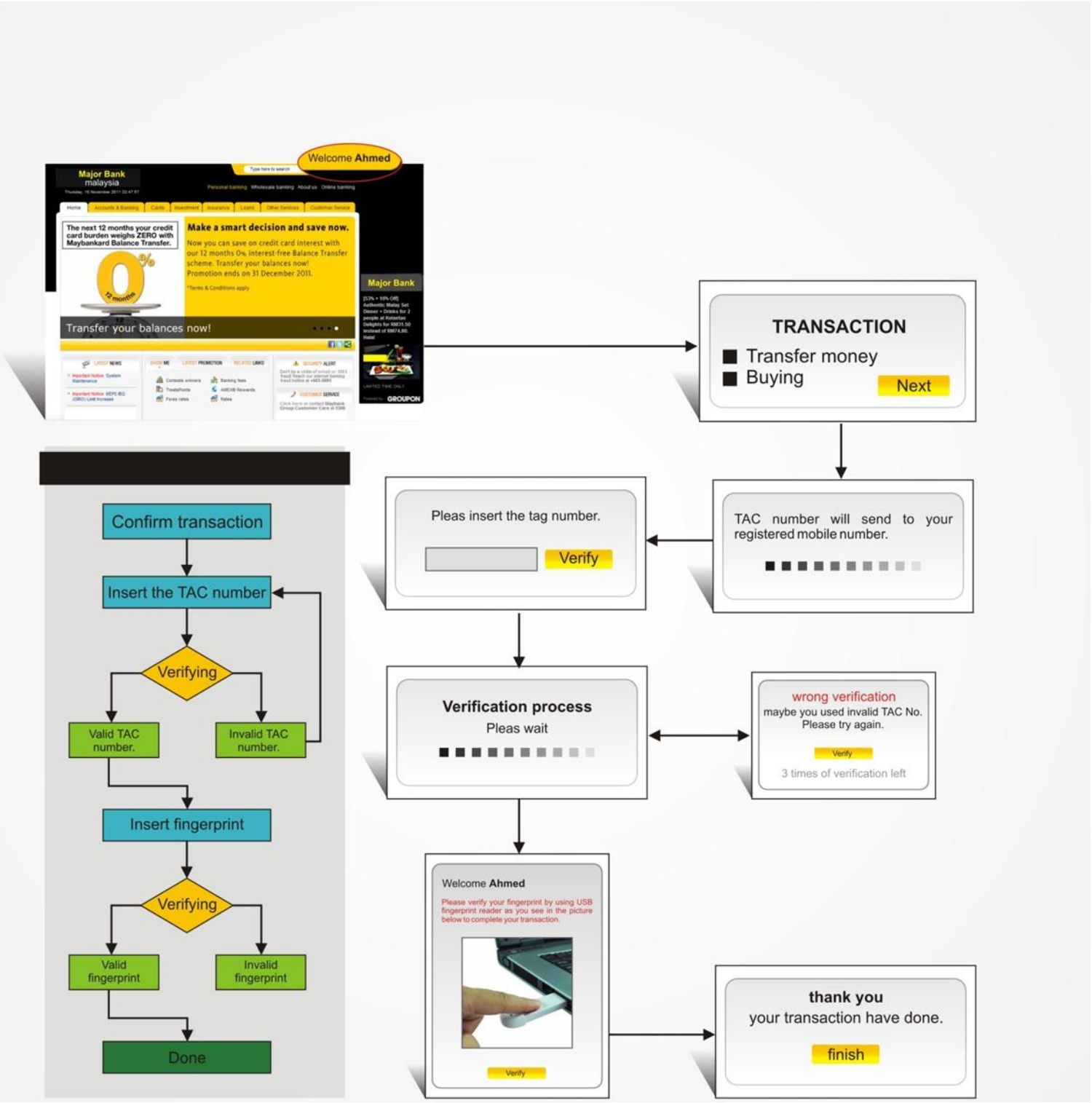

Figure 2. Authentication processes of transaction

B. Authentication processes of transaction

This process consists of two stages of authentication that the customer needs to confirm his/her transaction first stage is by using TAC, second one is by using biometric fingerprint technology (Figure 2).

Authentication process by using Transaction Authorization Code (TAC), e-banking system will send TAC automatically to the customer's mobile number, which is registered in the database of the bank system. The customer will receive text message (SMS) includes on Transaction Authorization Code (TAC). Therefore, after inserting the TAC the system will verify it, if it is accepted the browser will direct the customer to confirm his/her fingerprint again to complete the transaction.

The confirmation processes of transaction should be very secure because it protected the customer account from unauthorized changing, editing, or writing. This process is called integrity which is required to protect the customer assets.

CONCLUSION

Information security is coming ubiquitous whether is logical or physical. It is an essential approach for every organization to protect its asset from intruders and malware. Most of the banks experienced many threats and abuse in their system. Information security ensures the confidentiality of information. The numbers of users of online banking has significantly increased; therefore, biometric fingerprint will be used to enforce the authentication and identification of the user with username and password as an approach. Researchers argued that biometric fingerprint is secure mechanism used to authenticate the person because password only verifies the username but not the physical identity such as person fingerprint. In addition, customers, employees are the weakest layer in information security.

As a result, policies will be utilized on how configure the device as well as training the people about awareness of security. The purpose of policy is to protect not only the company asset from threats whether internal or external but also to reduce cost and eliminate legal liability to employees. This paper will give the researchers the insight about biometric as the powerful tool and perfect solution for authentication.

REFERENCES

[1] M. I. Abbadi & M. Alawneh. "Preventing Insider Information Leakage for Enterprises", The Second International Conference on Emerging Security Information, Systems and Technologies, IEEE journal, pp. 99-160, DOI: 10.1109/SECURWARE.2008.14, 2008.

[2] A. Andress. Surviving security, 2004.

[3] R. Ayoub & C. Rodriquez. "A Best Practices Guide to Fingerprint Biometrics: Ensuring a Successful Biometrics Implementation", White paper, 2011. Retrieved Nov., 2011 from: http://www.frost.com/prod/servlet/cpo/240303611

[4] S. Debbarma & S. Das. "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System". IJICT Journal, Volume 1 No. 5, pp. 197-203, 2011.

[5] A. J. Harris & D. C. Yen. "Biometric authentication: Assuring access to information", Information Journal of Management and Computer Security, Emerald Group Publishing Limited, 10(1), 12-19,2002.

[6] L. Harris & L. J. Spence. "The ethics of e-banking". Journal of Electronic Commerce Research. VOL. 3, NO. 2,2002.

[7] D. Hutchinson & M. Warren. "Security for Internet banking: a framework", Logistics Information Management, Emerald Group Publishing Limited, 16(1), pp.64 – 73, 2003.

[8] P. Jones. "Biometrics in retailing", International Journal of Retail & Distribution Management, Vol. 35 No. 3, 2007 pp. 217-222, 2007.

[9] C. K. Karlof. "Human Factors in Web Authentication", University of California, Berkeley, Technical Report No. UCB/EECS-2009-26, 2009. Retrieved Oct., 2011 From: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-26.pdf

[10] S. Liu & M. Liu. "A Practical Guide to Biometric Security Technology", IEEE Journal, 3(1), PP. 23-32, 2001.

[11] E. Maiwald. Fundamentals of Network Security, 2004.

[12] M. Merkow & J. Breithaupt. Information Security: Principles and Practices, 2006.

[13] J. E. Mills, M. Meyers, & S. Byun. "Embracing broad scale applications of biometric technologies in hospitality and tourism: Is the business ready?", Journal of Hospitality and Tourism Technology, Emerald Group Publishing Limited, Vol. 1 No. 3, pp. 245-256, 2010.

[14] M. Nami. "E-Banking: Issues and Challenges", ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009.

[15] N. C. Sickler & S. J. Elliott. "An evaluation of fingerprint image quality across an elderly population vis-a-vis an 18-25 year old population", IEEE, PP. 68-73, 2005.

[16] R. Tassabehji & M. A. Kamala. "Improving E-Banking Security with Biometrics: Modelling user attitudes and acceptance", IEEE Journal, pp. 1-6, DOI: 10.1109/NTMS.2009.5384806, 2009.

[17] S. Venkatraman & I. Delpachitra. "Biometric in banking security: A case study", Information Journal of Management and Computer Security, Emerald Group Publishing Limited, 16(4), 415-430, 2008.

[18] P. E. Proctor. The Secured Enterprise Protecting your Information Asset, 2002.