A Proposed Biometrics Technologies Implementation in Malaysia Internet Banking Services

M.K. Normalini and T. Ramayah

Abstract The security risks of Internet banking have always been a concern to the service providers and customers. One of the main issues related to Internet banking in Malaysia is the weak security of the Internet banking application. Therefore this study will investigate further the solution to enhance the security issues in Internet banking services by proposing the biometrics technology implementation. In this work we begin by analyzing user authentication methods being used currently in Internet banking, in order to propose a multi layered authentication technique which integrates to suit different Internet banking services based on risk assessment criteria's and other constraints. Multi-layered authentication in the Internet banking context refers to the requirement of multiple login names, passwords, and biometrics factors. Many systems utilize a combination of these methods in order to increase the level of security. Thus, a possible option is to introduce biometric authentication.

Keywords Internet banking • Biometrics • Security • Authentication • Phishing

1 Introduction

The Malaysian banking sector is under the supervision of Bank Negara Malaysia and is licensed under the Banking and Financial Institutions Act 1989 (BAFIA). The sector includes commercial and merchant banks, finance companies, discount houses and money brokers which act as financial intermediaries (BNM 2009). The banking sector accounted for about 70 % of the total assets in the financial system at the end of 1999 and is the primary source of financing for the domestic economy. The sector comprised of 27 commercial banks (19:100 % owned by foreign entities and 8:100 % owned by local entities) in the year 2012 (BNM 2012). Thereafter, there was a merger of domestic banking institutions which significantly reduced the number to ten commercial banks, ten finance companies and nine merchant banks. Currently, about 75 % of the banking sector's market share (total assets and total

M.K. Normalini (✉) • T. Ramayah
School of Management, Universiti Sains Malaysia, Penang, Malaysia
e-mail: normalini_mk@yahoo.com; ramayah@gmail.com

M.H. Bilgin et al. (eds.), *Innovation, Finance, and the Economy*, Eurasian Studies in Business and Economics 1, DOI 10.1007/978-3-319-15880-8_7

deposits) are controlled by domestic banking institutions (excluding the discount houses) (BNM 2009).

The banking sector is being transformed by developments in telecommunications and information technology. Electronic banking has become the ultimate service delivery system to fulfill the needs of banking customers due to the explosive expansion of the Internet and computer usage. The Malaysian government has structured a legal framework for Internet banking services as a result of the competitive nature of the banking sector.

The Malaysian Central Bank authorized domestic commercial banks on first of June 2000, to offer Internet banking services. The largest domestic bank in Malaysia, Maybank, became the first Malaysian bank to offer Internet banking services on June 15th 2000. By the seventh of August 2002, eight Malaysian commercial banks started providing Internet banking services, including Alliance Bank, Ambank, Bumiputra-Commerce Bank, Hong Leong Bank, Malayan Banking, Public Bank, RHB Bank, and Southern Bank (Suganthi and Balachandran 2001).

In Malaysia, adoption of Internet banking is comparatively low and the main determinants for adoption have not been researched much. This can be supported by Zanariah et al. (2012) and Raman et al. (2008) who categorized Malaysia as among the developing countries and the recent statistics show that the adoption of Internet banking in Malaysia is still low in spite of various initiatives made by financial institutions to attract users. Despite all the advantages of Internet banking, studies by Mohan et al. (2013) and Noorizan et al. (2012), suggests that general usage of Internet banking is still not in line with the growth of the Internet banking services in Malaysia. Hence, Internet banking development is still at the early phase though the electronic transformation has begun in Malaysia. Furthermore, the banking industry is finding it difficult to improve the dissemination of Internet banking (Ndubisi and Sinti 2006).

2 Malaysia Internet Banking Threats and Issues

There are a few security issues occurring in Malaysian Internet banking such as Online Identity Fraud or Phishing. *Phishing* or online pilfering of identity is the malevolent attempt of baiting mass audiences into misleading websites by thousands of emails sent by fraudsters. Criminals create websites that appear to be from trusted organizations and blast deceptive emails to random email addresses in an attempt to commit online identity fraud or *Phishing*. Connections to websites that appear to be similar to the websites of real organizations deceive customers into providing precision information such as user IDs, passwords, and TACs. Criminals are able to access the customer's bank account by using this personal information.

MyCERT or the Malaysian Computer Emergency Response Team operates a public service in the form of the Cyber999 Help Centre which provides emergency response to computer security issues in addition to support in management of incidents such as computer abuses, hack attempts and other security breaches

Table 1 MyCERT security breaches (2005–2010)

	2005	2006	2007	2008	2009	2010
Harassment	43	63	68	72	174	419
Fraud	149	287	364	907	1,022	2,212
Malicious code	82	68	182	277	283	1,199
Denial of service	7	6	8	12	28	66
Intrusion	467	897	385	766	1,766	2,160
Total	748	1,321	1,007	2,034	3,273	6,056

Source Data taken from MyCERT (2010)

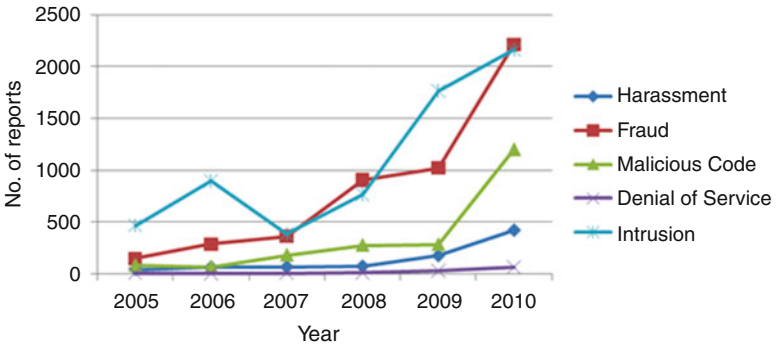

Fig. 1 Security breach trends for all categories

related to confidential information. The summary report of MyCert Security Breaches (2005–2010) relating to computer security incident handling and trends observed from the research network provides an overview of activities carried out by MyCERT (2010). Incidents categories supported by MyCERT (from 2005 to 2010) are shown in Table 1 and Fig. 1.

By and large, all categories show increasing trends in the number of reports every year. The majority of incidents recorded were due to fraud and intrusion representing 37 and 36 % respectively for the year 2010, followed by malicious code at 20 %, harassment at 7 % and denial of service at 1 %. Incidents related to system intrusion were generally caused by web defacement. The major reason for defacements was discovered by MyCERT to be related to vulnerable web applications. Phishing sites of local and foreign institutions comprised most of the fraud related incidents (MyCERT 2010). There is a variation of data availability by category as precise definitions of cyber security data categories that are currently used by the CERTs are difficult to find. Furthermore, many countries do not have national CERTs even though these institutions are often the main sources of such cyber security data. In addition, CERTs are relatively new in several countries and most do not provide much data. Exploring cyber international relations will be a challenge if inadequate data availability continues.

3 Internet Banking Security

Internet banking users are steadily increasing not only in Malaysia, but all over the world. Internet banking facilities which provide 24/7 services was convenience and gives an edge over other delivery channels such as phone banking, fax banking, and kiosk through dedicated lines to the bank. Overall, Malaysians were accepted Internet banking happily to solve their daily banking transactions in very minimum time. However, there are some issues with Internet banking which needs to be dealt with. Malaysians and banking customers were need to be concern and aware about the issues in Internet banking applications even though the issues are big in nature. According to Ooi (2002), the main issue is on trusting the Internet banking due to security reasons. Generally, this section will discuss about security policy guideline in Internet banking in Malaysia. Finally, the propose Internet banking security mechanism framework is suggest to enhance the security issues occurs.

Meanwhile, Tan and Teo (2000) determined that a very important factor in Internet banking adoption was risk. Ndubisi et al. (2004) on the other hand found that raising public confidence for system utilization involved the important aspect of security adequacy. Poon (2008) examined ten factors (convenience; accessibility; feature availability; bank management and image; security; privacy; design; content; speed; fees and charges) influencing e-banking adoption in Malaysia and found that security, privacy and convenience were significant contributors to e-banking acceptance. Even though the studies presented earlier found that e-banking offers new possibilities, a number of crucial psychological and behavioural factors have to be dealt with. These are trust, security, reluctance to change and human interaction preference factors.

4 Biometrics Technologies Implementation

A biometric is defined as "a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee" (Khosrow-Pour 2007, p. 53). Biometrics is a well-known technique to identify an individual or verify its identity (Mahier et al. 2009). Biometric technology provides a range of automated methods which can be used to measure and analyze a person's physiological and behavioral characteristics (Alhussain and Drew 2009). It usually involves a scanning device and related software which can be used to gather information that has been recorded in digital form.

According to Pranic et al. (2009), their research results showed that travelers perceived that some security measures such as sky marshals, fingerprints, eye scans, and face scans were both acceptable and effective at airport security. Therefore, making the distinction between biometrics' acceptance and perceived effectiveness, the implementation of biometric technologies at airports is an inducement for all stakeholders to understand this important issue from the technology point of

view and from the consumers' point of view (Pranic et al. 2009). Meanwhile, biometric technologies are perceived as acceptable and effective in the grand scheme of improving security in the overall flying process.

Several biometric traits have been proven useful for biometric recognition (Faundez-Zanuy 2009). Currently, the common used biometric systems include fingerprint, iris, face, and voice recognition. The world has entered the age of universal electronic connectivity so that people's daily life has a close relationship to various "e-things", such as e-commerce, e-library, e-government, and so forth. In such an e-world, more and more activities should be related to security services. With rapid progress in electronic and Internet commerce, there are now hand-held devices with the ability to be secure. Companies have also now offer a portable fingerprint reader for the Compaq, HP and Casio hand-held units where a customer can choose authentication with or without a smart card (Zhang 2002) (Fig. 2).

There are many industries that using biometrics implementation such as banking, immigration, national identity, telephone systems, time, attendance and monitoring and covert surveillance. Immigration authorities throughout the world are pressure by the issue such as terrorism, drug trafficking, illegal immigration, and an increasing throughput of legitimate travelers. It is essential that these authorities

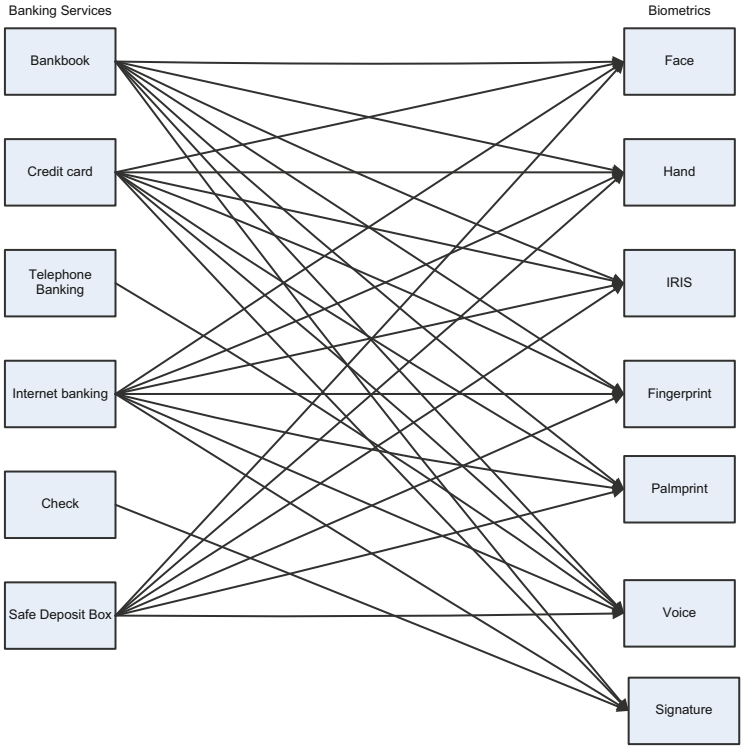

Fig. 2 Potential biometrics applications in banking

can quickly and automatically process law-abiding travelers and identify the law breakers. This is possible by being employed biometrics implementation.

Biometrics is beginning to assist governments as they record population growth, identify citizens, and prevent fraud occurring during local and national elections. Often this involves storing a biometrics template on a card that in turn acts as a national identity document. Finger scanning is particularly strong in this area. Biometrics technologies are not something new in Malaysia since the government sector has implemented in National Registration Department or (JPN), which represents the largest user of biometrics. Mykad as identity card keep biometrics data through embedded microchips. Besides, the immigration department has implemented the auto gate system installed at various entry points of the country and airport as authentication system by using thumb print scanner to match with passport embedded microchips, which keep biometric data. Financial institutions such as traditional banking also require thumb print scan to authenticate each risk transaction.

Communication has become accessible worldwide in the past 10 years with simultaneous advances in technology and reduction in communication costs. However, there has also been increasing vulnerability faced by telephone companies due to escalating fraud which have damaging effects on companies and their customers. Companies are now turning to biometrics technology to defend against such onslaught after the success of this technology in other security related issues. One such example is using 'Speaker ID' technology which is a technique based on voice recognition of people and is well suited for application in telephones and the communication industry. At present, certain factories and companies use punch cards to keep track of employee movement, whereby cards have holes punched into them when inserted into a machine as employees arrive and leave the company. Such a system can be abused and would therefore benefit from biometrics technology with the use of a system that requires employees to scan their fingerprints before arriving or leaving. The effectiveness of biometrics technology has given rise to evolving application and new challenging areas such as using biometrics for covert surveillance. With developments in facial and body recognition technologies, biometrics can even be used to automatically identify notorious suspects entering buildings or passing through crowded security sensitive areas such as airports. However, technical challenges such as concurrently identifying multiple subjects amongst hundreds of people and dealing with difficult subjects have to be resolved when using biometrics for covert identification as opposed to authentication. Biometrics devices used for this purpose will have to be able to recalibrate for inconsistent poses, viewing angles, or distances from the detectors.

According to Zhang (2002), biometrics applications are not limited to the areas already mentioned. In fact, the most common method to identify suspects and bringing criminals to justice by law enforcement community which are matching fingerprint images or parts of palm images.

Biometrics industry has been tremendously growing in developed countries like US and Japan. There are many gadgets being introduced in those countries to facilitate the current lifestyle. The cardless payment system should be replaced and there must be more easier, reliable, secure, cash free, and tension free payment system such biometric payment system in which no one has to carry a dozen cards for shopping, travelling, entering office, passing university entrances or bank door locks, entering Internet online shopping, and various kinds of card systems installed (Kumar and Ryu 2009). The research conducted in Sweden by Brobeck and Folkman (2005) showed that companies believe that biometrics is for organizations with a very high security need. Furthermore, the result showed that individuals are positive towards biometrics. Finger-scan is the technology most known of, trusted and preferred, for most likely, because it is a mature identification technique that has been around for a long time.

There has been increasing research done on biometrics such as the study by Al Harby et al. (2008) which found that the majority of Saudis prefer to use fingerprint identification methods and biometrics authentication systems using fingerprints are now practically and culturally accepted by Saudis (Al Harby et al. 2010b). Another research conducted by Al Harby et al. (2010a) involved using the technology acceptance model for prediction on acceptance of using biometric authentication systems in the online banking environment.

Past literature have shown the acceptance and biometric technologies implementation, and it has already been implemented in certain government departments, issues like it is something new and impossible to implement in other areas should not be brought up, and these technologies are growing to enhance the security level of authentication system.

5 Conclusions

In this paper, a proposed solution regarding the combination of biometric factors and traditional password technologies to increase levels of security in online applications such as Internet banking. Malaysia is moving towards becoming a developed country by the year 2020, it is believed that biometrics could be a key driver of growth for Malaysia. From the perspective of significance of biometric technologies, global needs, and national needs, which are in alignment, Malaysia can contribute and even lead the biometric technologies as to accomplish the mission. As the Malaysian government has always emphasized on security and privacy protection in financial, economic, political transactions, it is undeniable that biometrics technology could contribute in achieving this aim.

References

Al Harby, F., Qahwaji, R., & Kamala, M. (2008). The feasibility of biometrics authentication in e-commerce: User acceptance. In *The IADIS international conference WWW/Internet,* Freiburg, Germany.

Al Harby, F., Qahwaji, R., & Kamala, M. (2010a). Towards an understanding of user acceptance to use biometrics authentication systems in e-commerce: Using an extension of the technology acceptance model. *International Journal of E-Business Research, 6*(3), 34–55.

Al Harby, F., Qahwaji, R., & Kamala, M. (2010b). Users' acceptance of secure biometrics authentication system: Reliability and validate of an extended UTAUT model. *Communications in Computer and Information Science, 87*(2), 254–258.

Alhussain, T., & Drew, S. (2009). Towards user acceptance of biometric technology in e-government: A survey study in the Kingdom of Saudi Arabia. *IFIP Advances in Information and Communication Technology, 305*, 26–38.

BNM. (2009). *Chapter three banking sector* [online]. Available at: http://www.bnm.gov.my/view.php?dbIndex=0&website_id=1&id=14. Accessed June 02, 2010.

BNM. (2012). *Annual report* [online]. Available at: http://www.bnm.gov.my. Accessed August 27, 2013.

Brobeck, S., & Folkman, T. (2005). *Biometrics: Attitudes and factors influencing a breakthrough in Sweden*. University of Jonkoping, Master thesis.

Faundez-Zanuy, M. (2009). Biometric security technology. *IGI Global*, *8*.

Khosrow-Pour, M. (Ed.). (2007). *Dictionary of information science and technology*. Hershey: Idea Group Reference.

Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. *International Journal of Advanced Science and Technology, 4*, 25–38.

Mahier, J., Pasquet, M., Rosenberger, C., & Cuozzo, F. (2009). Biometric authentication. *IGI Global*, *9*.

Mohan, H., Ahmad, N., Chi Kong, Q., Tzeh Yew, C., Liew, J., & Nik Mat, N. K. (2013). Determinants of the internet banking intention in Malaysia. *American Journal of Economics, 3*(3), 149–152.

MyCERT. (2010). *Malaysian computer emergency response team report* [online]. Available at: http://www.mycert.org.my/en/services/statistic/mycert/2009/main/detail/625/index.html. Accessed June 10, 2010.

Ndubisi, N. O., & Sinti, Q. (2006). Consumer attitudes, system's characteristics and internet banking adoption in Malaysia. *Management Research News, 29*(1/2), 16–27.

Ndubisi, N. O., Sinti, Q., & Chew, T. M. (2004). Evaluating Internet banking adoption in Malaysia using the decomposed theory of planned behavior. In *The international logistics congress proceeding, Izmir*, 2004.

Noorizan, M. M., Raja Munirah, R. M., & Norfazlina, G. (2012). Perceived trustworthiness and the behavioral intention to use internet banking service among bank users in Shah Alam, Selangor. In *The international conference on innovation, management and technology research, ICIMTR2012*, Malacca, Malaysia, 2012.

Ooi, J. (2002). *E-banking is here to stay*. Kuala Lumpur: New Straits Times Press.

Poon, W. C. (2008). Users' adoption of e-banking services: The Malaysian perspective. *Journal of Business & Industrial Marketing, 23*(1), 59–69.

Pranic, L., Roehl, W. S., & West, D. B. (2009). Acceptance and perceived effectiveness of biometrics and other airport security procedures. *Acta Turistica Nova, 3*(1), 1–22.

Raman, M., Stephenaus, R., Alam, N., & Mudiarasan, K. (2008). Information technology in Malaysia: E-service quality and update of internet banking. *Journal of Internet Banking and Commerce, 13*(2), 1–18.

Suganthi, B., & Balachandran, P. (2001). Internet banking patronage: An empirical investigation of Malaysia. *Journal of Internet Banking and Commerce, 6*(1).

Tan, M., & Teo, T. S. H. (2000). Factor influencing the adoption of internet banking. *Journal of the Association for Information Systems, 1*(5), 1–44.

Zanariah, Janor, H., Rajendraan, E., Khamis, N., & Shamsuri. (2012). Internet banking: Analysing encouragement and impediment factors among academicians. *International Journal of Computer Networks and Wireless Communications (IJCNWC), 2*(3), 335–341.

Zhang, D. D. (2002). *Biometric solutions for authentication in an e-world* [online]. Available at: http://books.google.com.my/books?hl=en&lr=&id=tEtMjF33jgYC&oi=fnd&pg=PR11&dq=biometric+implementation+in+online+application&ots=wsp166059M&sig=RPvk-t_6-F2sQsjuuV-76wxMCo4#v=onepage&q=&f=false. Accessed October 02, 2010.