PROTECTING BANK CUSTOMERS PRIVACY IN ONLINE BANKING

[1]EBUBEOGU AMARACHUKWU FELIX, [2]ANUSIONWU CHINONSO KINGSLEY, [3]AKANWA CHINEDU SMITH, [4]ELILERICHARDUGOCHUKWU, [5]NWAOZUZU UDOCHUKWU GODWIN

[1]University of Malaya 50603, Kuala Lumpur, Malaysia
[2]MAHSA University 42610 Jenjarom, Selangor Malaysia
[3]Universiti Kuala Lumpur 50250 Kuala Lumpur Malaysia
[4]Limkokwing University 63000 Cyberjaya, Selangor Malaysia
[5]Kuala Lumpur Metropolitan University College 50350 Kuala Lumpur Malaysia
E-mail: [1]felixbosken@siswa.um.edu.my, [2]chinos4u@gmail.com, [3]chinedu.smith@s.unikl.edu.my, [4]Richard.mba16@grad.putrabs.edu.my, [5]Nwaudowin@hotmail.com

Online banking providers must be very dynamic in responding towards enhancing the security issues faced by their customers. Obviously internet banking applications should be protected in such a way that unauthorized access cannot be allowed to temper with customers private data. Banks are expected to improve more on the part of security issues as part of the benefits to their customers. Despite all the noteworthy achievements in addressing the security issues faced by online banking providers, security issues have not been fully addressed. The application of artificial intelligent systems such as biometric based applications have to some extent, but, not fully addressed the issue of security as well privacy. These intelligent systems restrict individuals from having access to vital data. A reliable internet system is expected to protect customers data including funds in their bank accounts. In this study, the security issue face on online banking is addressed, to restore consumer integrity on internet banking. A layered authentication method is applied to achieve the objective. The results indicates that bank customers are more concerned with their privacy and security. The results further suggests that even if a customer loses his or her online banking credentials that the customersprivacyisassured.Thisstudyisexpectedtoserveasblueprintformoresecurityapproachesinonlinebankingservices.

Keywords - Bank Customers, Online Banking, Privacy, Security, Multi-Level Authentication

I. INTRODUCTION

In developing countries like Malaysia, with the rapid tech- nological advancements and increasing consumer demands for more efficient delivery services, the financial landscape has continued transition towards increased level of significance of Internet banking as one of banking distribution channels (Portela Thanassoulis, 2007). However, in recent years, the financial services industry has been characterised by increased global competition, the transition from paper-based to elec- tronic products, and a raft of regulatory changes. The relentless march of technology has allowed banks to extend the scope of their activities and increase their operational efficiency, automating critical functions such as credit checking and loan approvals. At the same time, the rapid growth of electronic payments has exposed the weaknesses of complex legacy batch-processing systems and prompted the adoption of new technologies that store and transfer critical information in real time, yet security challenges with in the online banking applica- tion has not been fully addressed. This digital revolution is also presenting new challenges in terms of ensuring data privacy and protecting customers from fraud across multiple service- delivery channels (Kaplan, Norton, et al., 1992), (Oliveira von Hippel, 2011), (Guillen Tschoegl, 2008), (Aladwani, 2001), (Jenkins, 2007). Against the backdrop of rapid technological progress, the changing behaviour of customers and target customers has become a critical consideration for banks. As the cost of PCs, processing power and memory continue to fall, customers are increasingly interacting with banks in a virtual world, as well as through more traditional channels such as branch visits and contact centre calls. As a result, banks that fail to innovate and compete effectively across all channels may risk losing market share to a new generation of tech- savvy competitors (Vrechopoulos Atherinos, 2009), (Xue, Hitt, Chen, 2011), (Babbie, 2013), (Xu, Benbasat, Cenfetelli, 2011), (Zeithaml, Parasuraman, Berry, Berry, 1990). In this environment, technological innovation is recognised as a key differentiator among banks today. Institutions in the west increasingly use technology, such as customer segmentation and accessibility software, to tailor services to the needs of specific customer groups, including older people, young people, or people with disabilities (Zeithaml Parasuraman, 2004). At the same time, banks in emerging markets are exploring the potential of online and telephone channels to de- liver services to rural, geographically-distributed populations in the most cost-effective way possible (Berndt, Bhat, Fisher, Hevner, Studnicki, 2004), (Cole, Purao, Rossi, Sein, 2005). The intangibility of banking services makes the evaluation of service quality and customer convenience difficult to measure. Bankers obviously recognize the importance of intangible factors, but because of pressures placed on operating mar- gins caused by the current economic climate and chronically low margins, the evaluation off actors related to quality of service becomes paramount for

bank managers. Bankers, by necessity, seek to promote improvement initiatives, which will assist banks in improving their perceived costumer portfolio quality. Such portfolio can be achieved if customers privacy is protected. This study aims to construct an integrated evaluation system for retail banking service quality and convenience at the bank branch level while assuring secured internet banking as a benefit to the customers. A secured authentication method is applied to ensure that customer privacy is protected even when the customer loses his or her online banking credentials. It is widely recognised that safe and efficient retail payment systems enhance the effectiveness of the financial system, boost consumer confidence and facilitate the functioning of commerce (Arbore Busacca, 2009),(Hoffman, Roesler, Moon, 2004), (Aarts, Verplanken, Van Knippenberg, 1998). The remainder of the paper is organised as follows, Section 2 presents clearly the problem overview of the current study and its objectives, Section 3 present the proposed approach. Section 4 presents the results and discussion. In Section 5 we present the conclusion.

II. PROBLEM OVERVIEW

It is crystal clear that most of the online banking frauds are conducted either through phishing, stealing of banking infor- mation or through cloning of credit/debit cards. In phishing, a fraudster will send an email pretending to be sent from the bank to the victim asking for their personal details including banking information like PIN code or banking user name and password on some pretext or the other. Once the person reveals such crucial information, the fraudster may withdraw or transfer the money from the account of the victim.

In most cases, due to lack of awareness, people fall for the traps of such fraudster and loses huge sums of amount. The hassle in internet banking transactions has discouraged most consumers from using this method. They would prefer to transact by cash or checks and this encourage consumers to remain as branch banking customers (Horlick-Jones Rosenhead, 2002), (Fer- reira, Santos, Rodrigues, Spahr, 2011), (Anderson Sullivan, 1993).

A. Objectives of the Current Study

Banks can achieve new competitive advantage by restoring trust and confidence in their customers through the use of multi-level security approach which the current study offers as the pace of technology change continues to increase. The objectives can be summarized as follows;

1. Quickly shore up defences of weak channels that could be exploited by fraudsters seeking out point of vulnerability
2. Adapt detection to new and morphing fraud patterns.
3. Flexibly address a diverse range of fraud management needs in the ways that makes the most sense for each purpose: build own solution with sourced components and tools, implement fully sourced on-site solution, access hosted solution, and as well extend existing solutions.
4. Adjust fraud management solutions to changing Banks structures and IT architectures.
5. Move towards customer-level fraud management strategies that consider the value of the entire customer relationships and adequate data security.
6. To help banks in keeping pace with technology change, which illustrates how banks can invest in their technology infrastructures today to control costs, increase back-office ef- ficiency, and improve customer satisfaction in the near future. Not only do bankers think their organizations are more in- novative, the industry is also recognizing the importance of innovation and making more of a commitment to that effort and now is the time to act. The proposed approach is expected to restore customers confidence at all times.

III. RESEARCHDESIGN

This section presents the proposed approach to secure customers private date in an online banking scenario. Figure 1 presents the research design which enabled us to device a means of achieving the set objectives.

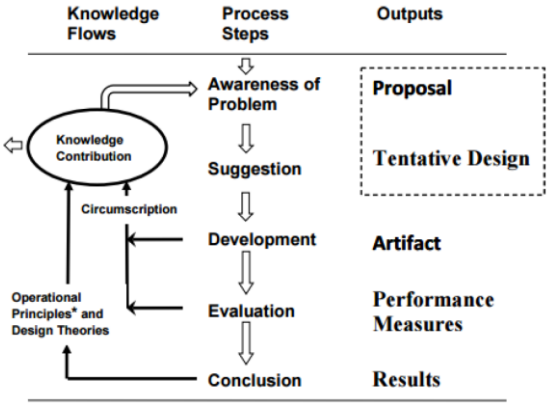


Figure 1. Research design Flow chart

The research design has three, the knowledge flows, process steps and the output phase. At the knowledge flows phase we structured the flow of process of the research design. The knowledge flow is the initial phase which serves as a guide to the research design. Its main components arethe researchers main ideas and contributions. The process steps elaborates on the awareness of the existing problem. At this phase, we established the problem being addressed in the current study. After the problem has been established, we proceed with suggestions and possible means of addressing the problem. Among the possible sets of solutions suggested, we then

focused on a single approach to address the problem, we then start the design of the proposed approach and evaluation. Every phase of the research design is accompanied by an expectedoutputasshowninFigure1.

IV. PROPOSEDAPPROACH

With the increase in online banking, it is imperative to en- sure that the applications used to deliver sensitive information on devices are secure. This is accomplished by architecturally hardening the application and requiring mutual authentication. This process makes data theft significantly more complex and costly for hackers. With new, sophisticated malware arriving daily, it is critical for financial institutions to ramp up secu- rity efforts against cybercrimes, and a layered approach will deliver the defence that ensures banking customers remain loyal, secure and safe as they engage in banking from more locations and types of devices than ever before. Therefore, the current research applies a mutual authentication approach in ensuring that customers data an effectively protected at all times across multiple electronic devices while accessing their online banking. The proposed approach is aim at ensuring a reliable quality of service, responsiveness, privacy and security control, quality assurance as shown in Figure2.These inde- pendent variables are

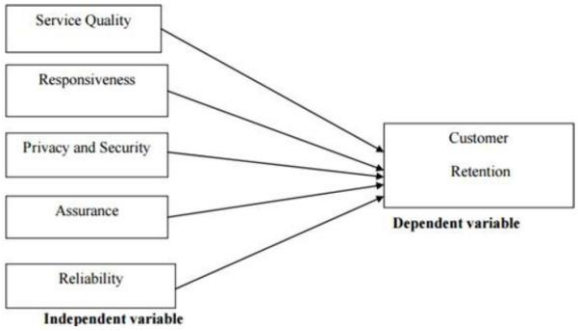


Figure 2. Proposed model framework

key to attend customers retention within an organization. The proposed approach takes into account these independent variable to meet the expected objective. Therefore, we propose possible prediction models built using the above independent variables to ensure that banks and other financial institutions maintain customers loyalty through a secured online banking process.

A. Regression Models

First regression model built as a function of quality of service as independent variable to ascertain the level of customers retention. Second regression model built as a function of responsiveness as independent variable to ascertain the level of customers retention. The third regression model built as a function of privacy and security as independent variable to ascertain the level of customers retention. Fourth regression model built as a function of assurance as independent variable to ascertain the level of customers retention. Fifth regression model built as a function of reliability as independent variable to ascertain the level of customers retention. Where CR is customer retention, QS is the quality of service, Rs is responsiveness, PS is privacy and security, A is assurance and Re is reliability. The reason for these above models is to clearly identify the correlation between each independent variable and the dependent variable We constructed the fowling regression model to ascertain among the independent variable the most concerned issues to ensure customers loyalty within the banking sector.

a. (CR → QS + error)
b. (CR → Rs + error)
c. (CR → PS + error)
d. (CR → A + error)
e. (CR → Re +error)

B. Hypothesis

We formulated the following hypotheses based on the proposed approach.

1. The quality of service can increase the chances of customer retention
2. Responsiveness can increase the chances of customer reten- tion
3. Privacy and security issues can result to a loss in customers retention
4. Assurance from the Bank can retain the bank customers
5. Reliability issue can result to a loss in customers retention Several banks customers were interviewed across Kuala Lumpur for instance, customers from Maybank, CIMBank, OCBC bank, AfinBank, Standard Chartered Bank and HSBC Bank.

V. EXPERIMENTATION

A. Data Collection

The bank customers were interviewed based on their online banking experiences. Forms were given out to the customers based on demography. The forms contains multiple question with the above independent variable to enable the customers express how they feel using the online banking applications. A reasonable amount of data was collected which enabled us to analyse the data collected accordingly.

B. Prototype

Furthermore, we designed a prototype of online banking application which was reviewed by the customers to compare with the existing application they use. The prototype was developed using ASP.NET, and the programming language used is C and the IDE used is Microsoft Visual Studio 2013 professional in designing the front end while the back end uses Microsoft SQL Server 2012. The flow chart of the authentication process is presented in Figure3.

VI. RESULTS AND DISCUSSION

From the results obtained, the factor which scored the high- est percentage in terms of customers retention is the privacy and security factor. Such that most customers believe that if their privacy is protected without any threat from unauthorized agents it will increase their level of trust and commitment with the use of online banking applications provided by their various banks. Table 1 presents the various scores in percentage obtained by the independent variables considered in the current study.

The quality of service as responded by the various bank customers is a concern in which most customers believed is their main concern. Only 10% of the total number of customers believed that QS is their most concerned issue. In terms of responsiveness of the online banking applications, 10% of the customers of various banks believed that there is a need for the online applications to be more responsive. Where as

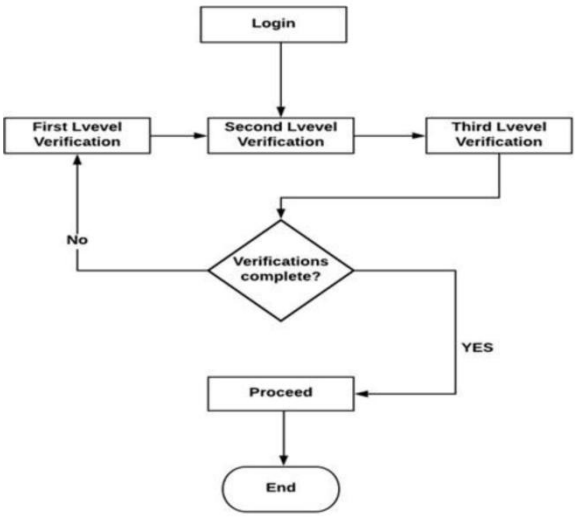


Figure 3. Login authentication process

Independent variables	Percentage score
QS	10%
Rs	10%
PS	45%
A	15%
Re	20%

TABLE I: Table 1 Scores achieved by independent variables

in terms of privacy and security, majority of the customers showed a huge concern over their privacy and security while using the online banking applications. Though most customers expressed their dissatisfaction on the rate of fraud associated with online banking in which some of the customers have been victims of online banking fraud. Of the total respondents, 45% of the customers strongly believe that the issue ofprivacy and security is of great importance while accessing the online banking applications. In terms of assurance, 15% of the total respondents agreed that the banking assurance is what they believe would keep their loyalty within their respective banks. Whereas in terms of reliability, 20% of the customers expressed their concern over the reliability of online banking applications. Figure 4 presents a bar chart showing thecorrela- tion between the various independent various considered inthe current study and the dependent variable. From the bar chart, it is very clear that the privacy and security factor indicated a very strong correlation with dependent variable and we can conclude that privacy and security issue has a strong and positive correlation with customers retention in the banking sector.

On the other hand, the login authentication designed was compare with the existing online banking login applications of various banks appears to have achieved a noteworthy remarks from the customers. If banks can implement multiple authentications for login, it will enhance the security and privacy standards in the online banking applications. A three level authentication is to ensure that the rightful owner of the account is verified accordingly to prevent unauthorized usage.

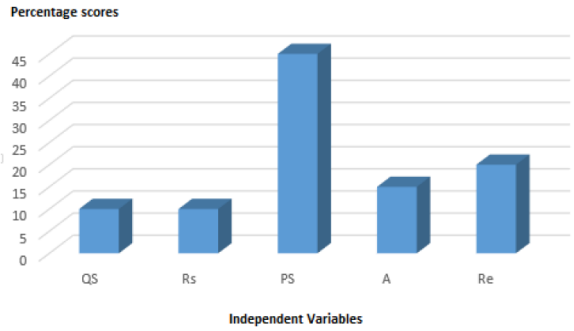


Figure 4. Percentage score of independent variables

Another advantage of the multiple authentication phase in the login process is that even if the customer loses his or her login credential or such credentials have been compromisedby fraud, their exist another level of authentication whichrequires to be verified before access can be granted into such online bank account.

VII. CONCLUSION

In this study, we have presented some independent variables like to help banks to focus more in protecting their customers in an online banking scenario. This study shows that the privacy and security of bank customers are the major concern and if improved, the customers loyalty will increase. This study further proposed a multi-level authentication technique which can be applied to improve online banking security. This technique will ensure that customers data is always protected even if the customer exposes his or her online banking credentials to an unauthorized person. Of the listed independent variables, the result indicates that most

customers are concern with privacy and security of their data including their bank account. In the future, we aim to investigate more factors which can be investigated to ensure that banks continue to improve on their customer retention approach and also to protect the privacy of their customers from fraud attacks.

REFERENCES

[1] Aarts, H., Verplanken, B., Van Knippenberg, A. (1998). Predicting behavior from actions in the past: Repeated decision making or a matter of habit? Journal of applied social psychology, 28(15), 13551374.

[2] Aladwani, A. M. (2001). Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information Management, 21(3), 213225.

[3] Anderson, E. W., Sullivan, M. W. (1993). The antecedents and consequences of customer satisfaction for firms. Marketing science, 12(2), 125143.

[4] Arbore, A., Busacca, B. (2009). Customer satisfaction and dissatisfaction in retail banking: Exploring the asym-metric impact of attribute performances. Journal of Retailing and

[5] Consumer Services, 16(4), 271280. Babbie, E. R. (2013). The basics of social research. Cengage learning.

[6] Berndt, D. J., Bhat, S., Fisher, J. W., Hevner, A. R., Studnicki,

[7] J. (2004). Data analytics for bioterrorism surveillance. In International conference on intelligence and security informatics (pp. 1727).

[8] Cole, R., Purao, S., Rossi, M., Sein, M. (2005).Being proactive: where action research meets design research. ICIS 2005 Proceedings, 27.

[9] Ferreira, F. A., Santos, S. P., Rodrigues, P. M., Spahr,

[10] R. W. (2011). Evaluating retail banking quality service and convenience with mcda techniques: A case study at the bank branch level (Tech. Rep.).

[11] Guillen, M. F., Tschoegl, A. (2008). Building a global bank: The transformation of banco santander. Princeton University Press.

[12] Hoffman, R. R., Roesler, A., Moon, B. M. (2004). What is design in the context of human-centered computing? IEEE Intelligent Systems, 19(4), 8995.

[13] Horlick-Jones, T., Rosenhead, J.(2002). Investigating risk, organisations and decision support through action research. Risk Management, 4(4), 4563. Jenkins, H. (2007). Adopting internet banking services in a small island state: assurance of bank service quality. Managing Service Quality: An International Journal, 17(5), 523537.

[14] Kaplan, R. S., Norton, D. P., et al.(1992).The balanced scorecard: measures that drive performance.

[15] Oliveira, P., von Hippel, E. (2011). Users as service innovators: The case of banking services. Research policy, 40(6), 806818.

[16] Portela, M. C. A. S., Thanassoulis, E. (2007). Comparative efficiency analysis of portuguese bank branches. Euro-pean Journal of Operational Research, 177(2), 12751288.

[17] Vrechopoulos, A., Atherinos, E.(2009).Web banking layout effects on consumer behavioural intentions. International Jour- nal of Bank Marketing, 27(7), 524546.

[18] Xu, J. D., Benbasat, I., Cenfetelli, R.(2011).The effects of service and consumer product knowledge on online customer loyalty. Journal of the Association for Information Systems, 12(11), 1.

[19] Xue, M., Hitt, L. M., Chen, P.-y. (2011). Determinants and outcomes of internet banking adoption. Management science, 57(2), 291307. Zeithaml, V. A., Parasuraman, A. (2004). Service quality.

[20] Zeithaml, V. A., Parasuraman, A., Berry, L. L., Berry,

[21] L. L.(1990). Delivering quality service: Balancing customer perceptions and expectations. Simon and Schuster.

★★★