International Journal of Computer Engineering and Information Technology

VOL. 9, NO. 10, October 2017, 225–232
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

User Perceived Secure Mobile Banking Service Provision Framework

Nambiro Alice Wechuli[1], Wabwoba Franklin[2] and Wasike Jotham[3]

[1, 2] Department of Information Technology, Kibabii University, Bungoma, Kenya

[3] Department of Library Services, Kirinyaga University, Kerugoya, Kenya

[1]alicenambiro@yahoo.com, [2]fwabwoba@kibu.ac.ke, [3]jothamwasike@gmail.com

ABSTRACT

The rapid development of mobile technology has resulted in the domination of mobile devices as the main channel through which people conduct most of their day-to-day activities. Several financial institutions are incorporating mobile banking and financial services as a key component of their growth strategy. However, the increasing capabilities that mobile technology offers have brought about a large number of security challenges to mobile banking. This calls for the need to equip financial institutions with a framework for assessing how secure the mobile banking services they provide are. Survey research design was carried out to determine the cyber-security challenges to mobile banking experienced in SACCOs in Kenya and the approaches used to minimize their impact to mobile banking service provision by SACCOs were evaluated. The study determined the cyber-security challenges to mobile banking. It also evaluated ways in which SACCOs ensure user perceived secure mobile banking service provision. A user perceived secure mobile banking service provision framework was proposed based on the findings. The proposed framework was put on test using experts and was found to be highly reliable. The framework provides means by which SACCOs can assess how user perceived secure the services they provide to their clients are.

Keywords: *Cyber-Attack, Cybercrime, Cyber Security, Mobile Banking, SACCO.*

1. INTRODUCTION

The rapid growth of mobile networks has enabled high adoption of mobile services in developing countries [1]. According to Baraka [2], the International Telecommunication Union (ITU) estimated that global mobile subscriptions were 6.8 billion at the end of the year 2012. This was bound to increase the use of mobile banking services worldwide [3]. Nowadays, mobile devices have become a natural extension of their users because the users are using them for doing their banking, sharing files and music, reading emails, staying in touch with their loved ones and ordering things online [4]. Savings and Credit Cooperatives (SACCOs) have seized the widespread use of mobile devices as an opportunity to connect with their clients. SACCOs provide a full range of financial services which include savings, credit, remittances and insurance. Mobile banking enables customers to carry out their banking actions anywhere, any time and at a lower cost [5]. The mobile banking services are offered across distances effortlessly using mobile networks [6].

Cyber security is a concern for all sizes of businesses in every industry, but more so for the sector of the financial services as stated in the [7]. The report further states that the main target of cyber-attacks is the status and vulnerability of the financial sector. Cyber-attacks cause disruption which result in loss of revenue and consumer confidence, reduced profitability, reputational damage, higher debt levels and currency devaluations, among other risks. [7] states that the financial sector is a prime target for cybercriminals because banks and financial institutions, SACCOs included are truly where the money is, regardless of whether the motivation is financial gain, geopolitical, or a combination. Cyber-attacks have increased in recent times and experts believe that if nothing is done urgently about it, severity of future attacks could be greater than what has been observed to date [8].

The Kenyan SACCO sector has over 45% contribution to the nation's Gross Domestic Product [9] therefore need to be protected from cyber-attacks. There exists no cyber-security framework for user perceived secure mobile banking service provision for SACCOs in Kenya. This is the reason for carrying out research on user perceived secure

mobile banking service provision in SACCOs in Kenya with an aim of modelling a framework for user perceived secure mobile banking service provision.

2. RELATED WORKS

SACCOs have the ability and opportunity to reach clients in areas that are unattractive to banks such as rural or poor areas [10]. Moreover, since SACCOs have the ability to advance loans at interest rates that are lower than those charged by other financial providers, they are an external financing predominant form for small and micro enterprises in most of the developing counties where Kenya is inclusive [11]. Thus, SACCOs have proved to be very important micro finance institutions for financial resources mobilization for various development activities. According to [12], 63% of the population in Kenya relies on the activities related to Co-operatives for their livelihood where over 250,000 benefit through direct employment.

2.1 Related Frameworks

There exist some frameworks related to mobile banking. First, there is the Mobile Banking Systems security model which was developed by [2] in Tanzania. In this model, confidentiality of data is enhanced through the use of message encryption. Also, Message Integrity is ensured by the use of message digests. Authentication measures and server security management policy is considered. The framework has well considered the importance of securing the mobile banking system in an effort to ensure secure mobile banking service provision. However, the human factor was not put into consideration especially the social engineering approaches used to overcome security measures put in place. Also, the budgetary constraints were not put into consideration in addition to human factor.

Another framework is the conceptual model of social engineering based attacks proposed by [13] which was intended to provide a medium to measure the impact of Social Engineering based attacks over individuals and organizations. The model describes the impact and possible safeguards for Social Engineering based attacks. However, the budget issues were not put into consideration. Also, the model did not undergo any validation.

3. RESEARCH METHODOLOGY

The study adopted the positivist philosophical position since the emphasis was on objectivity. In the philosophy, positivist research was used due to its objectivity, generalization, and the separation of the researcher's influence to the actual activities being studied [14]. The researcher's role was limited to gathering the data that helps in understanding the situation in the studies researched.

In this study, survey research design was adopted. The survey research design as defined by [15] is a method of collecting information by interviewing or administering a questionnaire to a sample of individuals. The information obtained was used to model the framework. Different types of procedures were used for collecting data from different sources hence triangulation that led to enhanced validity and reliability of the data and its interpretation [16].

Cronbach's alpha coefficient was used to measure the reliability of the measurement scale where the measurement of the variables were found to be highly reliable with alpha coefficients which were greater than 0.70 which is the minimum acceptable Cronbach's alpha coefficient. Cyber security challenges to mobile banking which formed the independent variable had Cronbach's alpha coefficient of 0.821 while ensuring user perceived secure mobile banking service provision which formed the dependent variable had Cronbach's alpha coefficient of 0.837. Both descriptive and inferential statistics were used in data analysis.

4. RESULTS AND DISCUSSION

Findings from the study were arrived at by the establishment of the cyber security challenges to mobile banking and the identification of ways used by SACCOs for ensuring user perceived secure mobile banking service provision. SACCOs in Kakamega and Kisumu counties in Kenya were used in the study.

4.1 Findings on Cyber-security Analysis and Ways of mitigating it in mobile banking

In the study, 94.74% of the questionnaires were filled and returned. The response rate was adequate according to [17] who state that a response rate of 70% and over is excellent.

Concerning the establishment of the cyber security challenges to mobile banking, which formed the independent variable in the study, the first research question was posed whether there was lack of

awareness on adverse effects of cyber security threats among SACCO employees and whether it was a challenge to SACCOs. 72.2% of the respondents disagreed while 27.8% of the respondents were in agreement. Another research question sought to find out whether customers who use mobile banking within the SACCOs do not seriously consider security messages sent to them by the SACCO. 61.1% of the respondents disagreed, 11.1% of the respondents stated that they were not sure while 27.8% of the respondents agreed to the fact that customers seriously consider security messages sent to them by the SACCO.

Another question sought to find out whether there was lack of sufficient technological infrastructure in SACCOs from which 88.9% of the respondents disagreed while 11.1% of the respondents agreed to the fact that there is lack of sufficient technological infrastructure. This implies that SACCOs have gotten used to the infrastructure they possess and work in their capacity to deliver services to their clients. Another question sought to find out whether security technologies an example installing and updating of antivirus software were not well implemented where all the respondents disagreed.

The study sought to find out whether employees who handle mobile banking aren't at all taken for professional development where 88.9% of the respondents disagreed while 11.1% of the respondents were in agreement. The study also sought to find out whether action cannot be taken against those responsible for cyber security attacks if reported by SACCOs where 33.3% of the respondents disagreed, 55.6% of the respondents were not sure and 11.1% of the respondents were in agreement. The study sought to find out whether there isn't enough capitation dedicated to mobile banking of which 88.9% of the respondents disagreed while 11.1% of the respondents were in agreement.

The study sought to find out whether vulnerability assessment on mobile banking system is not done where all the respondents disagreed. The study sought to find out whether SACCOs lack cyber security policies on mobile banking system where all the respondents disagreed. Also, the study sought to find out whether SACCOs do not have well-defined strategies to address the cyber security risks of which all the respondents disagreed. The study sought to find out whether SACCOs receive complaints from customers stating that they received messages requiring sensitive information from a source which purported to be their SACCO where 77.8% of the respondents disagreed while 22.2% of the respondents agreed. The study also sought to find out whether SACCOs receive complaints from customers stating that they received calls requiring them to submit sensitive information from a source which purported to be their SACCO in which 77.8% of the respondents disagreed while 22.2% of the respondents agreed.

Concerning the establishment of the ways SACCOs ensure user perceived secure mobile banking, which formed the dependent variable in the study, the first question was posed whether authenticity of users is considered by SACCOs where all the respondents were in agreement. The study also sought to find out whether there was character masking on mobile banking application when a user types in the PIN where all the respondents disagreed. The study also sought to find out whether the PIN used in mobile banking application contains a combination of numbers, letters and symbols where all the respondents were in disagreement.

The study sought to find out whether users of the mobile banking application were encouraged by SACCO to periodically change their PIN where all the respondents were in disagreement. The study also sought to find out whether the mobile banking application logs out a user after a given time of idling in which all the respondents agreed. The study sought to find out whether login attempts on the mobile banking application were tracked where all the respondents agreed. Also, the study sought to find out whether there was transactions tracking and all the respondents agreed. The study sought to find out whether there are limits set to certain transactions such as withdrawing a certain maximum amount of money from an account where all the respondents were in agreement. Then, the study sought to find out whether no account changes in terms of amount of money are made to a user's account other than by the user himself/herself where all the respondents agreed.

Also, the study sought to find out whether SACCOs send warning messages related to cyber insecurity in mobile banking to their clients where all the respondents agreed. The study sought to find out whether telecommunication service providers ensure service availability of the mobile banking application for the SACCOs and all the respondents agreed. Also, the study sought to establish whether the mobile banking application automatically locks after a given number of password guessing where all the respondents were in agreement. Finally, the study sought to establish whether there is information recovery in case of loss where all the respondents agreed.

Though in the responses using frequencies, no major challenge was observed in the SACCOs by IT experts, the correlation results in the next section

indicate the challenges do exist. This may be due to the fact that IT specialists tend to work with challenges day in day out that they may not think of them being unique challenges.

4.2 Correlation between Cyber Security Challenges and User Perceived Secure Mobile Banking Service Provision

A correlation was performed between the challenges to mobile banking and user perceived secure mobile banking service provision at the 95 percent confidence level first in the absence of the moderating variables then in the presence of moderating variables. The mobile banking cyber security challenges which were correlated with the user perceived secure mobile banking service provision were lack of awareness on adverse effects of cyber security threats, inadequate technology, insufficient technical skills, inadequate legislation, insufficient funding, inadequate risk management plans and social engineering practices. The Correlation coefficient (r) and the level of significance (p-value).

When a correlation was carried out between the challenges to mobile banking and user perceived secure mobile banking service provision in the absence of moderating variables, lack of awareness on adverse effects of cyber security threats had a statistically significant negative correlation (r = -0.629 and p-value = 0.005, which is less than 0.05) with user perceived secure mobile banking service provision. This implies that when mobile banking system users are not aware of the adverse effects of cyber security threats, then cyber-crimes will be committed whether knowingly or unknowingly and in turn, the level of user perceived secure mobile banking service provision declines and thus requires intervention. Also, when there is awareness of the adverse effects of cyber security threats, the mobile banking system users may not seriously consider the security messages sent to them by the SACCO. Inadequate technology had a statistically significant negative correlation (r = -0.565 and p-value = 0.015, which is less than 0.05) with user perceived secure mobile banking service provision. This implies that if a SACCO does not keep pace with the changing technology, then the level of user perceived secure mobile banking service provision decreases. Also, if security technologies like installing and updating antivirus on the systems is not implemented, then the level of user perceived secure mobile banking service provision declines.

Insufficient technical skills had a statistical significant negative correlation (r = -0.500 and p-value = 0.034, which is less than 0.05) with user perceived secure mobile banking service provision. This implies that when the staff are not taken for professional development on technical skills on handling mobile banking, the level of user perceived secure mobile banking service provision declines. Legislation had a negative correlation (r = -0.073 and p-value = 0.774, which is greater than 0.05) with user perceived secure mobile banking service provision. Lack of legislation was not significant with secure provision of mobile banking.

Insufficient funding had a statistically significant negative correlation (r = -0.747 and p-value = 0.000, which is less than 0.05) with user perceived secure mobile banking service provision. This implies that when there is inadequate capitation dedicated to mobile banking the level of user perceived secure mobile banking service provision reduces and thus security in mobile banking should be given priority. Inadequate risk management factors had a statistically significant negative correlation (r = -0.583 and p-value = 0.011, which is less than 0.05) with user perceived secure mobile banking service provision. This implies that when there is lack of vulnerability assessment on mobile banking system and no cyber security policies exist, then the level of user perceived secure mobile banking service provision decreases. Also, when there aren't well-defined strategies to address cyber security risks, it leads to patchy implementation of existing policies resulting in a decline in the level of user perceived secure mobile banking services provided.

Social Engineering practices had a statistically significant negative correlation (r = -0.564 and p-value = 0.015, which is less than 0.05) with user perceived secure mobile banking service provision. This implies that when mobile banking service users receive calls and messages requesting for confidential information and they give out the information, then user perceived secure mobile banking service provision is not guaranteed.

An investigation was then carried out to determine whether moderating variables had any moderating effect on the relationship between the independent variable which is mobile banking cyber security challenges and the dependent variable which is user perceived secure mobile banking service provision. The analysis was performed using first order partial correlation analysis. The moderating variables were qualification of the respondent and the experience the respondent has. The First order partial correlation coefficient ($r_{xy.z}$) and the level of significance (p-value) were determined.

A correlation was carried out on lack of awareness on adverse effects of cyber security threats against

user perceived secure mobile banking service provision factoring the moderating factors where the moderating variables significantly moderated the relationship. Qualification of the staff has a significant slightly negative moderating effect ($r_{xy.z}$ = -0.634, p-value = 0.006) with the experience of staff having a significant moderately positive moderating effect ($r_{xy.z}$ = -0.563, p-value= 0.019). This implied that the presence of the qualification of the staff suppresses the relationship while the experience of the staff improves the relationship.

A correlation was carried out on inadequate technology against user perceived secure mobile banking service provision factoring the moderating factors which significantly moderated the relationship. Qualification of the staff had a significant slightly positive moderating effect ($r_{xy.z}$ = -0.561, p-value =0.017) with the experience of staff having a significant moderately negative moderating effect ($r_{xy.z}$ = -0.608, p-value = 0.010). This implied that the presence of the qualification of the staff improves the relationship while the experience of the staff suppresses the relationship.

Also, a correlation was carried out on insufficient technical skills against user perceived secure mobile banking service provision factoring the moderating factors where they significantly moderated the relationship. Qualification of the staff had a significant slightly negative moderating effect ($r_{xy.z}$ = -0.505, p-value = 0.039) with the experience of staff having a significant moderately negative moderating effect ($r_{xy.z}$ = -0.521, p-value = 0.032). This implied that the presence of both the qualification of the staff and the experience of the staff suppresses the relationship.

A correlation was carried out on insufficient funding against user perceived secure mobile banking service provision factoring the moderating factors where the moderating variables significantly moderated the relationship. Qualification of the staff had a significant slightly positive moderating effect ($r_{xy.z}$ = -0.746, p-value = 0.001) with the experience of staff having a significant moderately positive moderating effect ($r_{xy.z}$ = -0.619, p-value = 0.008). This implied that the presence of the qualification of the staff and experience of the staff, both improves the relationship.

A correlation was carried out on inadequate risk management plans against user perceived secure mobile banking service provision factoring the moderating factors where the moderating variables have a moderating effect on the relationship. Qualification of the staff had a significant slightly positive moderating effect ($r_{xy.z}$ = -0. 580, p-value = 0.015) with the experience of staff having moderately positive moderating effect ($r_{xy.z}$ = -0.409, p-value = 0.103) which was not significant. This implies that the presence of the qualification of the staff and experience of the staff, both improves the relationship.

Finally, a correlation was carried out on social engineering practices against user perceived secure mobile banking service provision factoring the moderating factors in which experience had a moderating effect on the relationship. Qualification did not have any effect on the relationship because it resulted into ($r_{xy.z}$ = -0.564, p-value = 0.018) with the experience of staff having moderately positive moderating effect ($r_{xy.z}$ = -0.460, p-value = 0.063) which was not significant. This implied that the presence of the qualification of the staff had no effect on the relationship while presence of experience of the staff improves the relationship. However, the level of significance is above 0.5 thus won't be considered in the development of the framework.

Based on the analysis results, the contribution of each mobile banking cyber security challenge to effective user perceived secure mobile banking service provision was determined from which a user perceived secure mobile banking service provision framework was proposed as presented in figure 1.

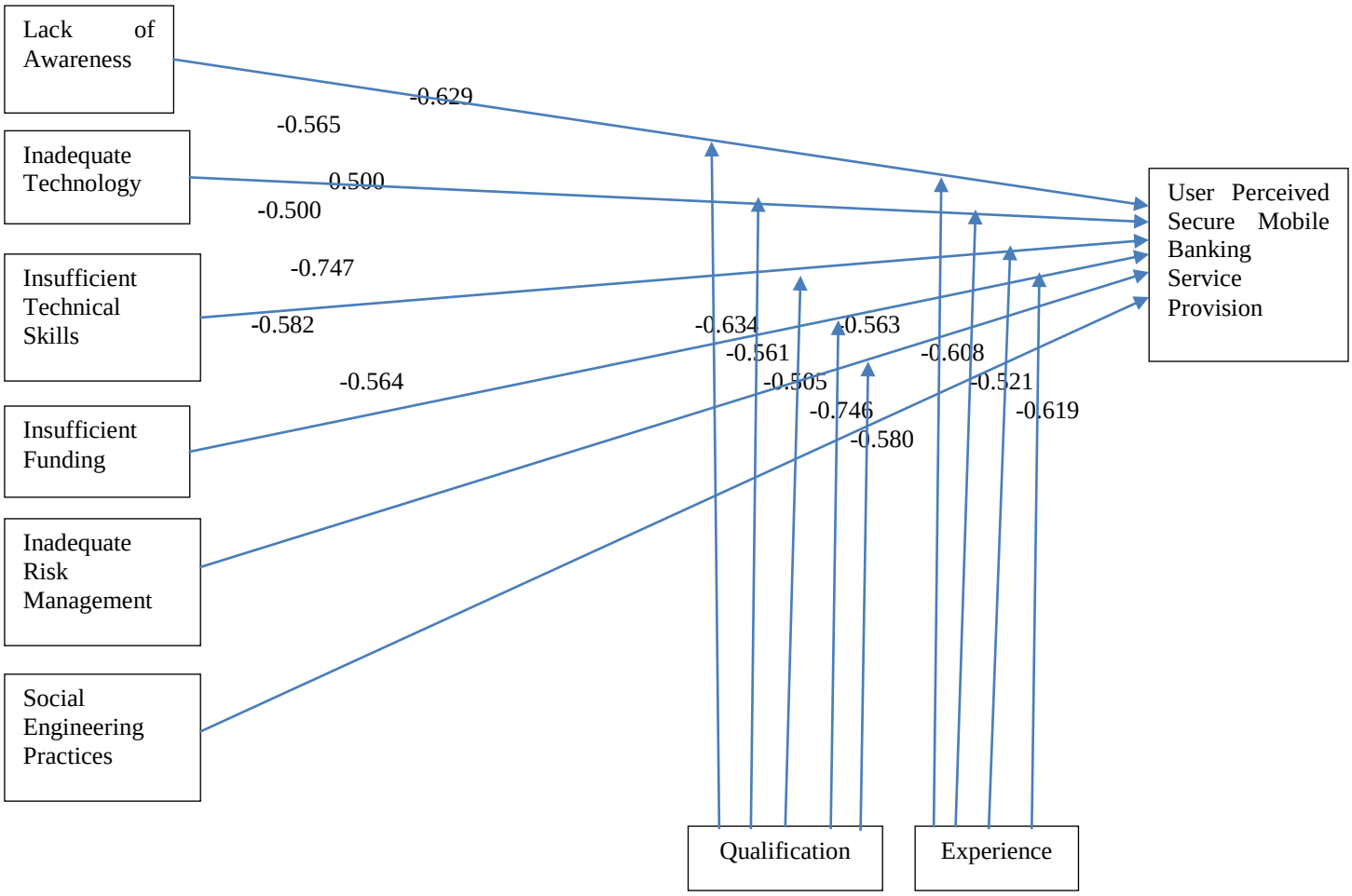

Fig. 1. Proposed User Perceived Secure Mobile Banking Service Provision (UPSMBSP) Framework

4.3 The Working of UPSMBSP Framework

The proposed user perceived secure mobile banking service provision framework shown in Figure 1 presents the measurement of secure services provided by mobile banking in line with mobile banking cyber security challenges for this research context. The results indicate that insufficient funding was the worst challenge posed in effective provision of user perceived secure mobile banking services in this research context. This implies that even if good plans are drafted but there are no funds to implement the drafted plans, they are rendered useless. Also, since technology is ever changing, embracing the new technology requires sufficient funds.

The second worst challenge that hinders effective provision of mobile banking services according to this context is lack of awareness on adverse effects of cyber security threats. This implies that even if the most current technology is employed by the SACCO but the users of the mobile banking system lack information on the effects of cyber threats, then they may knowingly or unknowingly leave the mobile banking system vulnerable to attacks.

The third worst challenge that hinders user perceived effective provision of mobile banking services according to this context is inadequate risk management plans. This implies that when the mobile banking system is successfully acquired and put into use but there are no policies guiding its effective use, no vulnerability assessment carried out on the system and lack of well-defined strategies to address cyber security risks then its continued existence is not guaranteed.

The fourth worst challenge that hinders effective provision of mobile banking services according to this context is inadequate technology. Since technology is always changing and new technology comes along with improved security features, failure to embrace the changing technology leaves the mobile banking system prone to attacks. Also, failure to implement security technologies exposes the mobile banking system to attacks.

The fifth worst challenge that hinders effective provision of mobile banking services according to this context is

social engineering practices. This basically deals with manipulating the human mind to give out sensitive information. This implies that when the mobile banking system users cannot differentiate legitimate information coming from the SACCO and the one posed by perpetuators, then they are prone to give out sensitive information to an attacker compromising the security of services provided. Therefore, education and training is key to ensuring user perceived secure mobile banking service provision.

The last challenge that hinders effective provision of mobile banking services according to this context is insufficient technical skills. This implies that even if the most current technology is embraced but there doesn't exist required technical skills to handle the system, then the system may most probably be exposed to attackers and in so doing compromises the secureness of the mobile banking services provided. The proposed framework was then validated using experts from SACCOs and was found to be highly reliable.

5. CONCLUSION

The literature reviewed on existing frameworks indicated that the frameworks had gaps in trying to address user perceived secure mobile banking. The proposed user perceived secure mobile banking service provision framework has delivered a solution to the problem of assessing how secure the mobile banking services provided by the SACCOs are. It is concluded that for user perceived secure mobile banking services to exist, cyber security challenges have to be addressed.

The study has several benefits to financial institutions, the telecommunication service providers, clients of the financial institutions, the research and the Kenyan government at large. To begin with, the study is of benefit to the mobile banking service customers of the banking institutions as they will get to know the ways in which social engineers use to deceive people into giving their sensitive financial information. Based on the information provided, they will be equipped to protect themselves from social engineering attacks on them by social engineers. The customers will be confident with the mobile banking services which will enable them enjoy the benefits of mobile banking.

The financial institutions will also benefit because they will offer better user perceived secure services to their customers that will increase the customer trust in mobile banking adding to the unbanked through this mode of banking hence increased revenue. Also, the Kenya government will benefit through the achievement of its cyber security objective of securing the citizens leading to improvement of productivity and hence increased tax returns. The increased tax collected will be used to improve the standards of living for the citizens in projects such as construction of roads in places where there is poor roads, construction of more public schools where schools are scarce, digging of boreholes in areas which face water scarcity and many more.

The mobile service providers will benefit from increased revenue as a result of increased transactions being conducted through the mobile banking services. Scholars will benefit from the studies, findings and contribution to the world of knowledge in the understanding of the cyber security measures that cab them in banking sector in Kenya. Finally, the researcher will benefit by obtaining the doctorate and in turn will contribute to the nation's manpower development in realizing sustainable millennium development goals.

ACKNOWLEDGMENT

We highly appreciate the National Commission for Science Technology and Innovation, Kenya for the study financial sponsorship.

REFERENCES

[1] Nicholaus, S.C. & Venkatakrishnan, V. Challenges of mobile-phone money transfer services' market penetration and expansion in Singida District, Tanzania. IRACST-International Journal of Research in Management and Technology (IJRMT), 3(6), 205-215, 2013

[2] Baraka W. N., Sam A., & Laizer L. S. Enhanced Security Model For Mobile Banking Systems In Tanzania. International journal of technology enhancements and emerging engineering research, 1(4), 2013

[3] Preeti S. & Prerna S. B. Issues &Challenges in Mobile Banking in India: A Customers' Perspective. Research Journal of Finance & Accounting, 2 (2), 2011

[4] GTISC, Emerging Cyber Threats Report 2012, Atlanta, GA, USA, 2011

[5] Esmaili, E. et al. The Role of Trust and Other Behavioral Intention Determinants on Intention toward Using Internet Banking. International Journal of Innovation, Management and Technology, 2(1), pp.95-100, 2011. Available at: http://www.ijimt.org/papers/111-E00102.pdf [Accessed January 3, 2012].

[6] Rumanyika J. D. Obstacles Towards Adoption Of Mobile Banking In Tanzania: A Review. International Journal of Information Technology and Business Management, 35 (1), 2015

[7] 2015 industry drill-down report (2015). Financial services

[8] Omondi, D. How fraudsters are sneaking into your mobile phone to steal private information. The Standard Newspaper, February 8th 2016

[9] Mumanyi, E. A. L. Challenges and opportunities facing SACCOs in the current devolved system of government

of Kenya: A case study of Mombasa County. International Journal of Social Sciences and Entrepreneurship, 1 (9), 288-314, 2014
[10] Olando, C. O., Jagongo, A. & Mbewa, M. O. The Contribution of Sacco Financial Stewardship to Growth of Saccos in Kenya. International Journal of Humanities and Social Science, 3 (17), 2013
[11] Kembo, M. B. & Mwakujonga J. Issues in SACCOS Development in Kenya and Tanzania: The Historical and Development Perspectives. Developing Country Studies, 3 (5), 2013
[12] Mudibo, E. K. Challenges and Opportunities Facing the Kenyan Savings and Credit Co-operative Movement. Presentation during the Africa Savings and Credit Co-operatives Conference 3rd - 6th October 2006 at the Grand Regency Hotel, Nairobi, Kenya, 2006
[13] Chitrey A., Singh D., Bag M. & Singh V. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. International Journal of Information & Network Security (IJINS), 1(2), 2012
[14] Wilford, S. H. "Information and Communication Technologies, Privacy and Policies: An Analysis from the Perspective of the Individual". Thesis submitted for the Doctor of Philosophy, De Montfort University, Leicester, UK, 2004
[15] Orodho, A. J. Essentials of Educational and Social Sciences Research Method. Nairobi: Masola Publishers, 2003
[16] Zohrabi M. Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings. Theory and Practice in Language Studies, 3 (2), pp 254-262, 2013
[17] Mugenda, O. M. & Mugenda, A. G. Research Methods: Quantitative and Qualitative Approaches. Nairobi: Acts Press, 1999.