Improving Mobile Money Security with Two-Factor Authentication

Adam B. Mtaho
Department of Business and Information Technology
The University of Dodoma
Dodoma, Tanzania

ABSTRACT

Security is a leading factor for establishing and maintaining customer trust in mobile money services (MMSs). MMSs in Tanzania rely on the use of Personal Identification Number (PIN) as an authentication method. However, a PIN can be easily guessed, forged or misused. This paper explores security challenges in MMSs and weaknesses associated with the current Mobile Money Authentication (MMA) method. Further, the study proposes the use of two-factor authentication model as an alternative method. The proposed model combines the current approach of using PIN and adds another layer of security that uses fingerprint recognition technology. Evaluation of the proposed model shows that it mitigates security vulnerabilities that exist in the current MMA method.

Keywords

Authentication, Biometric, Fingerprint, Mobile Money Services, PIN, Two-Factor Authentication

1. INTRODUCTION

Security is an essential factor for the success of MMSs. If customers are not assured to get secure services, they are likely to leave their service provider and thus risk the reputation of the industry as a whole [1].Wide acceptance and popular use of MMSs address the need to have secure mobile money systems. Mobile money technologies offer several services to customers. Three major services offered include money transfer, mobile banking and mobile payment. With money transfer service customers can send and receive money to each other. Mobile banking offers a convenient way of carrying out bank services such as money deposit and withdrawal, balance inquiries, etc. Mobile payment enables customers to pay for numerous services such as utility bills, school fees, and taxes and even to do online purchases. In order to secure provision of MMSs, any customer who accesses service in his/her mobile money account must first be authenticated. That is each mobile money customer who declares to own mobile money account must be verified to determine whether he/she is, in fact, the one who claims or is declared to be.

So far the MMA method that is used by all Mobile Network Operators (MNOs) in Tanzania is a Personal Identification Number (PIN). Each customer's mobile money account is linked to this PIN, which is unique and is limited to only one user. Before a user accesses any MMS, he/she is required to prove his authenticity by entering the PIN. If the entered PIN is correct, access to MMS is granted; otherwise access is denied. Despite its popular usage, studies have shown that the use of PIN as an MMA method has several security weaknesses. Some of those weaknesses include: PINs used are only four digits in length, thus they are likely to be easily guessed and forged. PINs are sent in plain text [2, 3] and are not masked while entered, which makes it visible for anyone nearby.

2. OVERVIEW OF MOBILE MONEY ACCESS TECHNOLOGIES

Unstructured Supplementary Service Data (USSD), Short Message Service (SMS) and Subscriber Identity Module (SIM) Toolkit-STK are three popular access technologies used in MMS in East Africa [4]. USSD is a protocol used in Global System for Mobile Communications (GSM) for supporting communication between mobile phones and service provider computers. USSD enables a real-time "session" to be initiated between the mobile user and the USSD application platform. When the service is invoked, it permits data to be sent back and forth between the mobile user and the USSD application platform until the USSD service is completed [5]. Once the session terminates the USSD application platform may be configured to allow an SMS to be sent to the user via Short Message Service Center (SMSC) in a GSM network. With STK, the user has an application on the SIM card that is accessed from the phone's menu [6].

3. SECURITY CHALLENGES THAT ARE ASSOCIATED WITH THE CURRENT MMA METHOD

This section reviews and present security challenges that are associated with the current MMA method.

3.1 USSD Technology Vulnerabilities

The use of USSD technology in MMSs conveys several security challenges. The PIN that passes via USSD technology to the server is in plain text; therefore attackers using network sniffers applications like Wire-shark can intercept it. Also, the service provider can read the sent PIN [2]. Moreover, USSD technology is vulnerable to malware attacks. Attackers have found ways to capture USSD codes and use that information to exploit Android devices [3, 7]. Some of Android applications can pass a USSD code to the dialer and execute USSD code directly without prompting it to the user [8]. These vulnerabilities on USSD technology can be used by attackers to access information stored in the SIM.

3.2 Mobile Phones Vulnerabilities

Mobile phone devices are now being used to store sensitive user's information such as bank details, confidential personal and business information, PINs, etc. They are also used to conduct several transactions such as money transfer, online purchase, bill payments etc. Apart from these services, some mobile phones such as smart phones are also expensive devices. Due to these attributes, mobile phones have therefore become the target of attacks. According to computer crime and security survey report of 2009, 42% of the respondents experienced "laptop and mobile hardware loss or theft" and 12% of these cases led to data breaches [9]. Viruses have also attacked mobile phone devices. According to the report by NISA [10], user's unawareness on smartphone might lead the user to install applications from non-trusted sources. These applications might contain malware that can alter private information in the smartphone or send private information to other devices. The information sent by malware can later be used by an attacker to conduct fraud in MMSs. Moreover, mobile phone has several security features that by default are left by the manufacturer without being activated. Some of these features allow encryption of the data, but this task is left to the user. If such features are not enabled, the online interception of the sensitive stored data such user's PIN is possible by the third party.

3.3 Mobile Money Customer Behavior

The customer who owns a mobile money account is accountable for maintaining security of his/her account. The manner in which mobile phones, SIM card and PIN are handled by the customer may affect security of the electronic money stored in mobile money account. For example, over trust of customer to mobile money agents such as telling them the PIN when the customer wants to withdraw money from mobile money account can lead to security breach. Sharing of mobile phones among family members and co-workers also may lead to unauthorized access of the mobile money account. The habit of charging many mobile phones at one place such as at the agent's office also adds more security risks, as it provides a room for a dishonest agent to access someone's mobile money account without being permitted by the owner.

3.4 Registration for MMSs

In order for a person to use mobile money account he/she must be registered using customer ID card. Types of identifications that are allowed include valid passport, employment ID, and an introduction letter from the village or ward executive officer (which must bear a full name and photograph of the applicant), etc. According to [11], registration process in MMSs creates more security vulnerabilities in many ways. For example, so far it is not possible to verify whether the ID card used for registering a mobile money customer was fake or real because mobile money agents have no special tools to verify those IDs. They just rely on inspecting the physical document without contacting the legitimate authority that provided it. This means that there is a possibility for a person to register with incorrect personal particular and perform any unauthorized transactions later without being identified [11].

3.5 Living and Working Environment

Usually mobile money business is done by agent separately or together with other services. Agent offices may have several staffs who serve for distinct services in the same office or shop. In case a dishonest staff who is not serving for MMSs knows the mobile money PIN of another staff who serves for MMSs, unauthorized transaction may be committed. The environments in which MMSs are carried are also subjected to security risks. For example, while some agents have permanent offices, other agents in town centers have no offices. They just stay along the road or near bus stands. Such environments make MMS vulnerable to theft or unauthorized access attacks. Unless strong authentication methods are used, security of MMSs will always remain at risk.

3.6 Personal Identification Numbers (PINs)

The current MMA method makes use of PIN to prove if the subscriber who performs a particular transaction is an authorized user. All MMSs such as money transfer; cash withdrawal and airtime purchase requires the use of PIN. The PIN used is too short (only 4 digits) which makes it easy for people to guess. Yet, such PIN is unmasked (written in clear text) therefore becomes more vulnerable for a snooping attack. The same PIN is used for authenticating a user for all MMSs. Sharing of PIN among users or family members also add more security risks. Studies [12-14] have reported that most users use their date of births as PINs. Such tendency leads to a critical security vulnerability as date of birth can be known from different sources, such as a co-worker, family member, relative, various record management systems etc. Also, currently there is no specific protection when user's mobile phone is stolen by fraudsters who can successfully figure out the user's PIN [3].

4. THE NEED FOR TWO-FACTOR AUTHENTICATION IN MMSS

The authentication methods used in computer systems are usually divided into three main types: those which are based on what a user knows (such as passwords, PINs, etc.), those which are based on what you have (e.g., credit card, master card, etc.), and those based on whom you are (i.e. biometric authentication which include fingerprints, iris scans, etc.). According to [9], although all three methods are used in authentication process, biometric authentication methods offer more benefits over other methods. So far users and agents of MMSs in Tanzania are authenticated by using PIN. A PIN is used to uniquely authenticate either an agent or customer whenever he/she wants to carry out any mobile money transaction. However, the "uniqueness "aspect of the PIN is "artificially" set because the PIN can be compromised. For example, the customer's PIN can be known by unauthorized user and hence be used for fraudulent purposes [14]. A robust authentication method is therefore needed to prevent unauthorized access of mobile money account. This study therefore proposes the use a two factor authentication (2FA) model for enhancing security in MMSs.

5. RELATED WORKS

Several studies have shown a great concern of security issues in mobile money services. Gilman et al. [1] highlighted several fraud cases that threaten the security of MMSs including false transactions, misuse of PINs and identity theft. The study found that MMSs operators are aware of the need to improve mobile money security and that improved security in MMSs will enable operators to protect themselves, their customers and agents, and assists successful provision of mobile money business.

The study by Intermedia [15] reported that 36% of mobile money users in Tanzania share their PINs that led to a great security risk. Of those who shared their PINs, 55% do so with agents while 45% share with close relations such as spouse, siblings and friends. The study argued that mobile money users who need assistance in processing transactions are more probable to share their PINs compared to users who do not need assistance. Another study [16] to identify security and privacy concerns of mobile money users in Africa revealed that if proper measures to secure mobile phones are not taken, mobile phone users might be vulnerable to criminal attacks.

Mangala et al. [17] proposed biometric method for providing the highest security to the mobile payment in e-banking particularly in wireless transmission level. In the proposed model, fingerprint image is taken in real time and sent to the server for authorization. A fuzzy logic based fingerprint matching algorithms are used in the server side for authorization.

Goyal et al. [18] designed a mobile payment system integrated with biometric authentication model that provides the facility of mobile payments with increased security levels. The proposed model would enable more people to use mobile payment system even with the simplest mobile phones from customer perspective. Aujla et al. [19] presented a secure account–based payment protocol that is suitable for m-commerce to transfer the payment from wireless networks based on public key cryptography.

According to [20], in order to enhance more security in authentication process, a combination of either of the two authentication methods, which is called two-factor authentication (2FA /TFA) can be done. Usually (2FA/TFA) involves something the user knows, for example a password and something the user has, possibly a smartcard or any other token and finally something the user "is" for example a fingerprint or voice pattern.

A number of studies [20-24] have proposed 2FA technique for security enhancement in mobile authentication. Most of 2FA combine two layers of security that includes "something you know" for example a password/username and "something you have" for example, a biometric feature like fingerprint or iris [25]. The study proposes the model for enhancing security in MMSs authentication by means of 2FA, which uses PIN and fingerprint recognition technology (FRT)..

6. THE CURRENT MMA MODEL

The current MMA model has two main phases, enrollment phase (as shown in figure 1) and Execution phase (as shown in figure 2). Before a user acceses MMS, he/she must first be enrolled. The enrollment phase invloves obtaining subriber's information including PIN, and saving that information including the PIN to the MNO server.

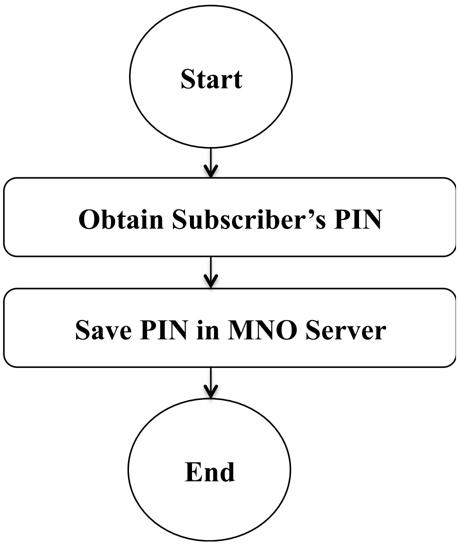

Fig 1: MMA Enrollment Phase

During the execution phase, in order to access MMS, user must initiate transaction by dialling a USSD code, selects a service from available service options, enters PIN and submit the request to the apropriate MNO's application server. The application server then authenticates the PIN, if the PIN is correct the requested service will be provided, otherwise the user will be given the opportunity to retry for the maximul of three trials.

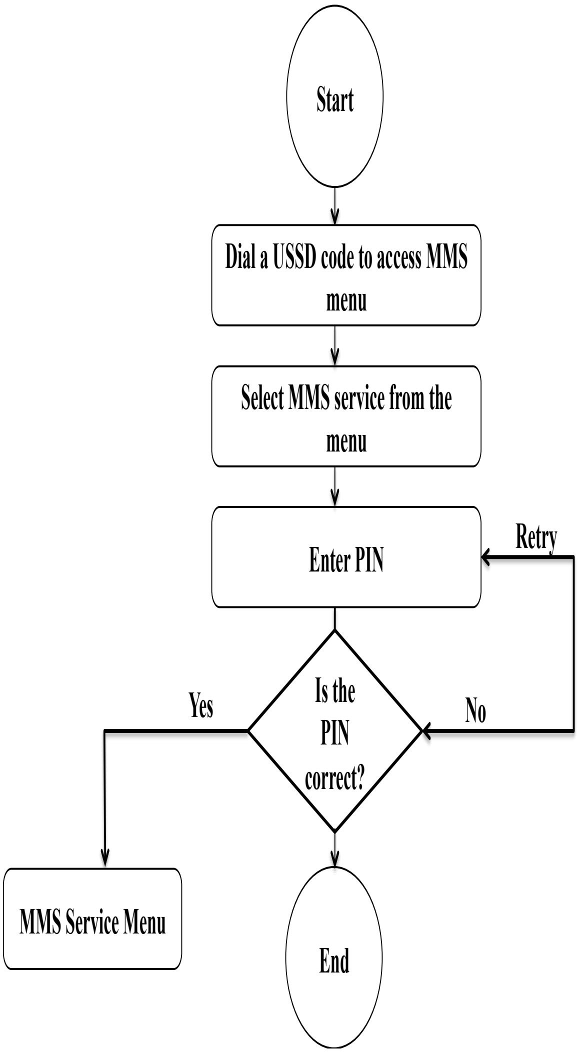
Start
Dial a USSD code to access MMS menu
Select MMS service from the menu
Enter PIN
Retry
Is the PIN correct?
Yes
No
MMS Service Menu
End

Fig 2: Execution Phase

The major drawback of this model is that if unauthorized user knows the customer's PIN and gets access to someone's SIM card, a fraudulent transaction can be committed from customer's mobile money account.

7. THE PROPOSED 2FA MODEL

In the proposed model, first, the user will be required to enroll his PIN and fingerprint and save that information in the MNO's server for future authentication. During the authentication phase, first the user will be authenticated by using the traditional model (PIN). Upon successfully authentication of the PIN, user will again be authenticated by FRT. The proposed model assumed that the smartphone used has embedded fingerprint recognition technology (for example Iphone 5s, Samsung Galaxy S5, Motorola Atrix 4G, HTC One Max and Huawei Ascend Mate 7). This model works in two main phases:

7.1 Enrollment Phase

This is the first phase whereby a user enrolls for MMSs. User enrolls his phone number and his PIN, which are saved in the MNO/s server. After that, user is required to enroll his fingerprint, which is scanned and saved as a template in the MNO server. The flowchart of the enrollment phase is depicted in figure 3.

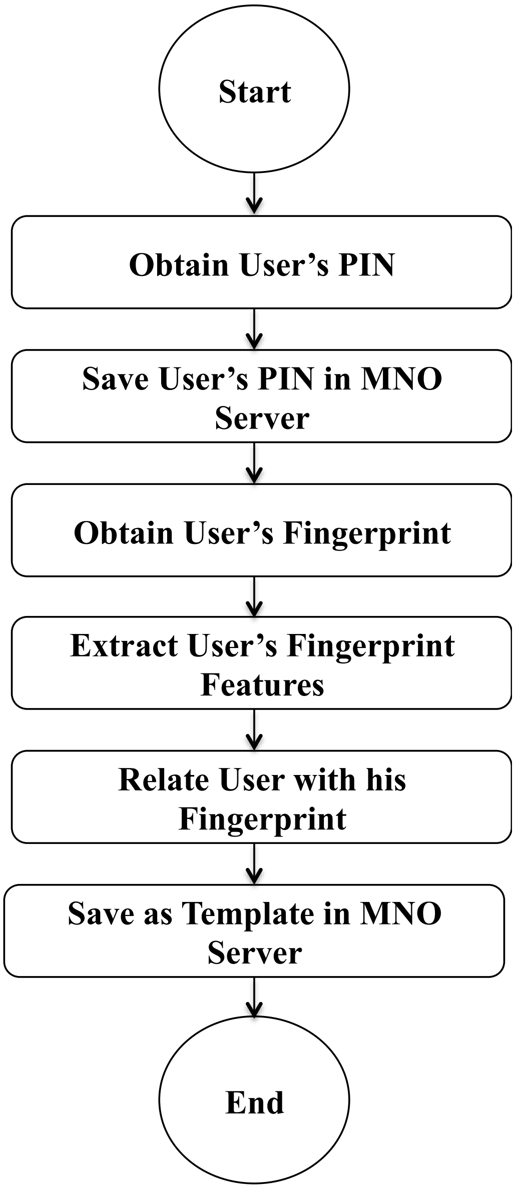
Start
Obtain User's PIN
Save User's PIN in MNO Server
Obtain User's Fingerprint
Extract User's Fingerprint Features
Relate User with his Fingerprint
Save as Template in MNO Server
End

Fig 3: Enrollment Phase in the Proposed 2FA Model

7.2 Authentication Phase

In this stage, user first accesses the MMSs menu by dialing a USSD code (example, *150*00#) and then enters his enrolled PIN. The PIN entered is sent to the server and cross-checked if it matches with the PIN already saved during enrollment. If the PIN matches user will be prompted to enter the fingerprint. The fingerprint is then scanned by the Smartphone's fingerprint recognition software and matched with the fingerprint template saved during enrollment phase. If the fingerprint matches, user will be given access to the MMSs menu. If the fingerprint does not match, access to the MMSs menu will be denied. The flowchart of the authentication phase is depicted in figure 4.

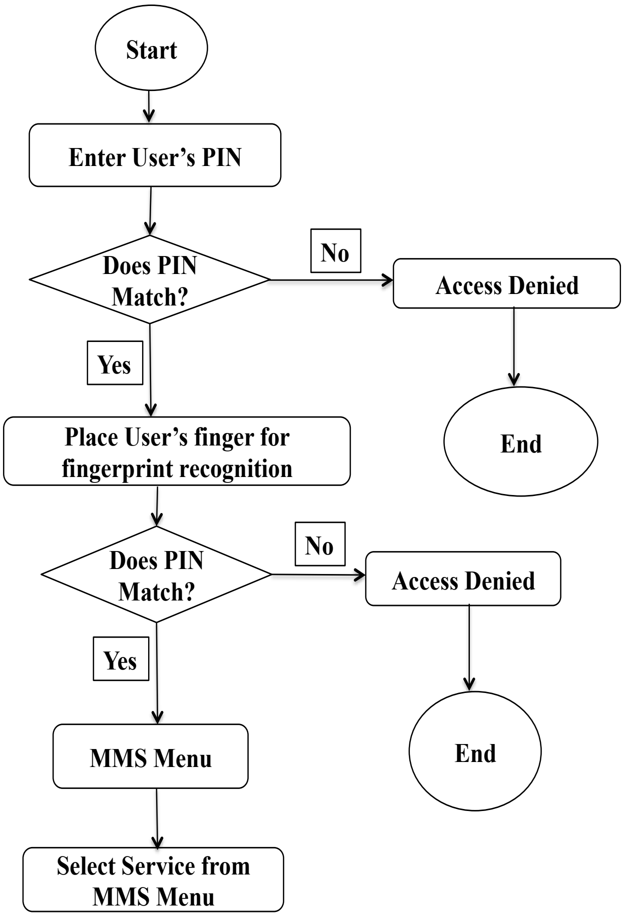

Fig 4: Flow chart for Authentication in the Proposed Model

A typical algorithm for the above model is show below:

Algorithm for the Proposed MMA model

```
Input: PIN, Biometric (Fingerprint)
Output: MMS Authorization
//$BT_F$: Fingerprint biometric
//BT: Biometric Template
//MS: Matching Score
//MSSA: Matching Score for MMS Authorization
//$PIN_{S:}$ Saved PIN in enrollment phase
// Enrollment Phase
Capture subscriber's PIN
Enroll the PIN in MNO server
Capture user's $BT_F$
Process the $BT_F$
Enroll the $BT_F$ in a MNO server
//Authorization Phase 1
Subscriber enters PIN
If (PIN=$PIN_s$)
        {//Authorization Phase 2
```

```
Subscriber enter $BT_F$
Live-scan subscriber's $BT_F$
Process the $BT_F$ and extract the $BT_F$
Compare the scanned $BT_F$ against the stored template
Provide a matching score to the application
        If (MS for BT1 ≥MSSA)
                Provide access
                else
                {Deny access}
                end if
else
end if
Log system usage pathway
```

8. EVALUATIONS AND DISCUSSIONS

In order to understand mobile money user's perception on the proposed 2FA model, a questionnaire method was used. The study employed purposively sampling technique whereby a sample of 50 respondents from three groups, of whom 9 were agents, 4 were MNO staff 37 were mobile money customers. The criterion used for selecting a customer or an agent is that, the respondent must have used/ or worked with MMSs for at least 6 months. In order explore more information relevant to the study, an interview with six key informants was also conducted, two from each group. Before distributing the questionnaire, participants were provided with an overview of the proposed model and present the weaknesses that exist in current MMA method. At the end, the participants provided their perception on the use of 2FA in MMSs. Participants gave their views based on the following questions: Will the use of 2FA eliminate unauthorized access in MMSs? Will the use of 2FA enhances security and freedom in accessing MMSs? Will mobile money users accept the proposed 2FA technology? Is the use of 2FA in MMSs convenience for users?

8.1 Data Representation from Questionnaire

Out of 50 distributed questionnaires, 50 were presented representing 100% of the total questionnaire administered. Respondents data presented here consist of demographic information, duration of MMSs usage, and perception towards the effectiveness proposed 2FA MMA model.

8.2 Demographic of the Respondent

As shown in figure 5, 52% of the total respondents were male and 48% of the respondents were female. According to age groups, 41% of the respondents were between 18 and 30, 30% were between 30 and 40 years, 23% were between 40 and 50 years and 6% were above 50 years.

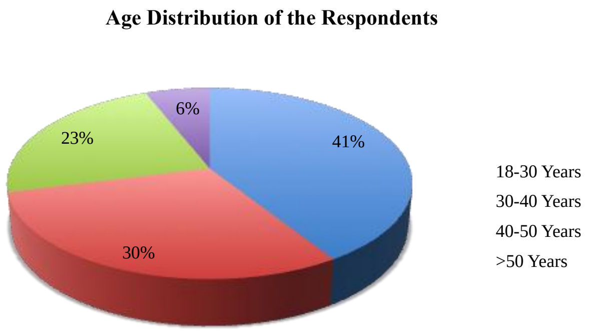

Fig 5: Age Distribution of the Respondents

8.3 Duration of MMSs Usage

Table 1 shows the duration of respondents in using MMSs.

Table 1: Respondents duration in using MMSs

Duration	Frequency
< 1 Year	15
1 – 2 Years	17
3 – 4 Years	18
Total	**50**

From Table 1, most of the respondents have been using MMSs for 3 to 4 years (36%). 34% of the respondents have been using MMSs for 1 to 2 years. 30% of the respondents have been using MMSs for less than 1 year.

8.4 Perception on the Effectiveness of the Use of 2FA in MMSs among Respondents

Respondents were asked to give their perception on the effectiveness of using 2FA in MMSs. The subscriber's perception on the effectiveness of the proposed 2FA model was obtained by using a five-point Likert scales ranging from 1-5. The scale options depended on the question, objective and on the fact measured. The scale ranged from Strongly Agree to Strongly Disagree. The response of the 50 respondents is as given in figure 6.

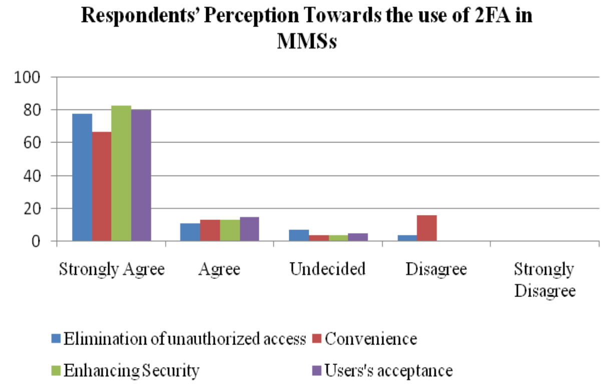

Fig 6: Respondents' Perception Towards the use of 2FA as in MMSs

8.4.1 Elimination Of Unauthorized Access To MMSs

Theft/loss of mobile phones contributes largely to the breach of financial data and illegal access to user's mobile money account. This always happens particularly if such incidents occurred for unprotected devices or for devices that rely heavily on the use of PIN as method of protection. During the study respondents were asked to provide the views whether the use of the 2FA with fingerprint technology will help eliminate the problem of unauthorized access to MMSs. From the study (as shown in figure 6), 78% of the participants strongly agreed that the use of 2FA will help eliminate the problem of authorized access to MMSs, 11% agreed, 7% were neutral (undecided) while 4 disagreed. This indicates that majority of respondents agreed that the use of 2FA in MMSs will help eliminate unauthorized access to MMSs. It was also urged by respondents that the use of fingerprint will offer more advantages over PIN since it is unique and cannot be easily forged. Therefore problems such as loss or theft of mobile phones which lead to unauthorized access will be eliminated because forging fingerprint is difficult.

8.4.2 Enhancing Security of MMSs

Mobile money services require higher level of security. This is because MMSs are carried out through portable computing devices which are subject to theft/ loss or snooping attack. Studies have shown that if customers are assured that mobile phone systems possess strong security mechanisms, they can even pay extra money for them in order to secure their businesses [26]. In this regard, during the study respondents were asked to provide their views whether the introduction of 2FA as a new MMA method in MMSs will help improve security in MMSs. As shown in Figure 6, 83% of the respondents strongly agreed that 2FA will enhance security in MMSs, 13% agreed and 4 were neutral. Therefore majority of participants viewed the use of 2FA to be secure. As already illustrated in the proposed model (figure 4), the user is firstly authenticated by PIN, and then by fingerprint. Thus, in case an attacker manages to forge a PIN; still he/she cannot access MMSs. Since fingerprint is unique from person to person, therefore cannot be impersonated. Such characteristics enable fingerprint-based authentication and identification systems to provide higher level protection than the conventional PIN method.

8.4.3 User Acceptance on the Use of 2FA in MMSs

The degree to which users accept the technology that supports a particular has direct impacts on its success. If MNOs release to the market the product or service which users will not accept it, there is the risk of not getting more customers or losing existing ones. In view of this, respondents were asked to give their views whether they will accept the proposed model once introduced as a MMA method. From the study it was found that 80% of the respondents strongly agreed that they are ready to use the proposed model if introduced, 15% agreed and 5% remained neutral. This indicates that majority of respondents accepted the use of the proposed 2FA model in MMSs. However, some respondents urged that since this model works only for mobile phones with fingerprint technology, its use will remain to be challenge task. This is because so far smartphones with FRT in Tanzania are still very expensive; therefore, majority of customers cannot afford to buy them.

8.4.4 Convenience of the 2FA Model in MMSs

Customers prefer to use the system that is not only secure but also convenient to use. Technological features such as convenience and ease of use have an influence on customer adoption on the product or service offered [26]. The respondents were asked to provide their views whether the proposed 2FA model is easy and convenient to use in MMSs. As shown in Figure 6, 67% of the respondents strongly agreed that 2FA is easy and user can operate it with convenience, 13% agreed, 4% remained neutral, 16% disagreed (saying that it will add more steps). This indicates that more than two-third of the participants' viewed the use of 2FA in MMSS as convenient method. It is true that adding another security layer after PIN means that processing time will also increase. However, compared to other biometric authentication methods such as person's voice, handprint, or retinal pattern; fingerprint verification is a quick and convenient method to use.

8. FUTURE

MMSs have revolutionized the way people are doing businesses. However, insecurity of MMSs has remained to be a major challenge for its adoption. This paper has explored security challenges in MMSs and weaknesses associated with the current MMA method; and have proposed the use of 2FA as an alternative solution. Future studies will focus on the cost benefit analysis of the proposed model. Further, this study has assumed that the proposed model will work with smartphones (which have embedded fingerprint recognition technology). Further study on how the proposed model can be applied to basic mobile phones is also needed.

9. CONCLUSION

This paper explores security challenges in MMSs and weaknesses associated with the current MMA method; and propose the use of two-factor authentication model as an alternative solution. Findings indicate MMSs are carried in the environments which are vulnerable to access attacks. The use of PIN as authentication method is vulnerable to illegal MMSs access. To address this problem, a 2FA model that uses PIN and fingerprint recognition technology has been proposed as an alternative. Evaluation of the proposed model shows that if this model is implemented, security of MMSs and customers' trust will be enhanced. MNOs are therefore advised to implement this model.

10. REFERENCES

[1] Gilman, Lara and Joyce, Michael. Managing the Risk of Fraud in Mobile Money. GSMA: Mobile Money for Unbanked (MMU). 2012.

[2] Chong, M.K., Security of Mobile Banking: Secure SMS banking. Data Network Architectures Group. University of Cape Town, South Africa, 2006.

[3] Alex Dobie.How to Tell If Your Samsung Phone is Vulnerable to Today's USSD Hack. Android Central, Retrieved 20 September 2014.

[4] ITU. The Mobile Money Revolution Part 2: Financial Inclusion Enabler. ITU-T Technology Watch Report. May 2013.

[5] Janagoudar Sanganagouda. USSD: A Communication Technology to Potentially Oust SMS Dependecy.Aricent.September 2011.

[6] Gunnar Camner, Caroline Pulver and Emil Sjöblom. What Makes a Successful Mobile Money

Implementation? Learnings from M-PESA in Kenya and Tanzania. GSMA.

[7] Vanja Svajcer. Not Just for PCs Anymore: The Rise ofMobile Malware. Sophos. 2014.

[8] Chuanxiong Guo, Helen J. Wang and Wenwu Zhu. Smart-Phone Attacks and Defenses.In: Proceedings of the 3rd Workshop on Hot Topics in Networks (HotNets). November, 2004.

[9] Robert Richardson. CSI Computer Crime and Security Survey. 2008.

[10] Smartphone: Information security risks, opportunities and recommendations for users, ENISA Report (December 2010).

[11] A. Basigie Mtaho and L. Mselle . International journal of Computer Science & Network Solutions. The electronic version of Securing Mobile Money Services in Tanzania: A Case of Vodacom M-Pesa, IJCSNS vol. 2, issue 5, 2014.

[12] Joseck Luminzu Mudiri. Fraud in Mobile Financial Services. Microsave, 2013.

[13] Joseph Bonneau, SorenPreibusch, Ross Anderson. A birthday presents every eleven wallets? The security of customer-chosen banking PINs. Lecture Notes in Computer Science Volume 7397, 2012, pp. 25-40.

[14] Harold F. Tipton, CISSP, Micki Krause. Information Security Management Handbook, Fifth Edition, CRC Press LLC, 2004.

[15] Intermedia. Tanzania Mobile Money Tracker Study: Wave 4 Report, InterMedia. March 2013.

[16] Harris, A, Goodman, S, &Traynor, P 2013, Privacy and security concerns associated with mobile money applications in Africa, 8 Washington Journal of Law, & Arts 245 (2013).

[17] Mangala Belkhede, Veena Gulhane, Dr. Preeti Bajaj. Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach. 1^{4th} International Conference on Advanced Communication Technology (ICACT), pp. 1193 – 1197, 2012.

[18] Jyotsana Goyal and Dinesh Goyal. Design of Improved Algorithm for Mobile Payments Using Biometrics. International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 6, Dec – January 2014.

[19] Pawandeep Singh Aujla and HarneetArora. A Secure Account based Mobile Payment Protocol with Public Key Cryptography and Biometric Characteristics. International Journal of Science and Research (IJSR), India, Online ISSN: 2319- 7064, March 2013.

[20] Karen Scarfone MurugiahSouppaya. Guide to Enterprise Password Management. 2009.

[21] F. Aloul, S. Zahidi, and W. El-Hajj. Two Factor Authentication Using Mobile Phones. IEEE International Conference on Computer Systems and Applications (AICCSA), Rabat, Morocco, 641-644, May 2009.

[22] Sagar Acharya, Apoorva Polawar, P.Y.Pawarn. Two Factor Authentication Using Smartphone Generated One Time Password. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278 - 0661, p - ISSN: 2278 – 8727, Volume 11, Issue 2 (May - Jun. 2013), PP 85 – 90.

[23] Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson. "Multi-Factor Authentication." U.S. Patent No. 20,130,055,368. 28 Feb. 2013.

[24] B. Schneier. Two-Factor Authentication: Too Little, Too Late. In Inside Risks 178, Communications of the ACM, 48(4), April 2005.

[25] T.Venkat NarayanaRao, Vedavathi K. Authentication Using Mobile Phone as a Security Token. International Journal of Computer Science Engineering and Technology (IJCSET). October, 2011, Vol 1, Issue 9, 569-574.

[26] Shon, T.-H., & Swatman, P. M. C. Identifying effectiveness criteria for Internet payment systems. Internet Research, 8 (3), 202-218, 1998.

[27] Nadarajah Manivannan, Celalettin Tigli, Azad Noor, Shahzad Memon. Fingerprint Biometric for Identity management. International Journal of Industrial Engineering and Management (IJIEM), Vol. 2 No 2, pp. 39-44, 2011