FACULTY OF ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING

ANINTEGRATION OF BIOMETRICS AUTHENTICATION INTO MOBILE MONEY SERVICES

KAKEMBO SAMUEL

BU/UP/2013/190

ACKNOWLEDGEMENTS

Great appreciation goes to the Almighty God, for giving me a gift of Life and a chance of education. I greatly appreciate my parents for the support, encouragement and motivation throughout my academic carrier.

I also thank my supervisor Mr. Lusiba Badru and the entire Department of Computer Engineering for the technical guidance throughout the execution of this project and my entire four years that I have spent in Busitema University.

DECLARATION

I, KAKEMBO SAMUEL do hereby declare that this Project Report is original and has not been submitted for any other degree award to any University before.

Signature……Date……

Name: KAKEMBO SAMUEL

Bachelor of Computer Engineering

Department of Computer Engineering

Busitema University.

APPROVAL

This Dissertation Report has been submitted with the approval of the following supervisor.

Signature. …….. Date……..……

Name: MR. LUSIBA BADRU

Department of Computer Engineering

Faculty of Engineering

Busitema University.

LIST OF ACRONYMS

GSM: Global Systems for Mobile communications

SMS: Short Message Services

SMSC: Short Message Service Centers

PIN: Personal Identification Number

USSD: Unstructured Supplementary Service Data

SIM: Subscriber Identity Module

STK: SIM Toolkit

MPOS: Mobile Point of Sale

MM: Mobile Money

MMS: Mobile Money Services

MMA: Mobile Money Authentication

MNO: Mobile Network Operators

UI: User Interface

API: Application Interface

IDE: Integrated Development Environment

SDK: Software Development Kit

XML: Extensible Markup Language

SQL: Structured Query Language

Open CV: Open computer vision

APK: Application Package

TABLE OF FIGURES

ABSTRACT

Security is a leading factor for establishing and maintaining customer trust in mobile money services (MMSs). MMSs in Uganda rely on the use of Personal Identification Number (PIN) as an authentication method. However, a PIN can be easily guessed, forged or misused. This report explores security challenges in MMSs and weaknesses associated with the current Mobile Money Authentication (MMA) method and a model integrated with biometrics authentication as an alternative.

The project aimed at integrating biometrics authentication into mobile money services to reduce mobile money fraud. It combines the current approach of using PIN and adds another layer of security that uses fingerprint recognition technology. Evaluation of the project shows that it mitigates security vulnerabilities that exist in the current MMA method.

Table of Contents

CHAPTER ONE: INTRODUCTION

1.1 Background

Mobile Money can be defined as an electronic wallet service, that lets users store, send and receive money using their mobile phones (both smartphones and basic feature phones).

It was first introduced in March 2009 and currently there are seven mobile money schemes in Uganda which include MTN Mobile money, Airtel Money, M-sente, Africell money, Zap, M-cash and Eeezy Money. It has been adopted by a number of user and currently standing at 18.5 million registered accounts, from a mere 10,011 accounts 7 years ago making it 53% of Uganda's population.

Mobile money offers enormous flexibility to customers as to deposit money as float onto their SIM card-based account which can later be converted into cash at any mobile money agent. In its initial stages, Mobile money was largely limited to person-to-person money transfer but with the growing interest from stakeholders, coupled with competition among the mobile network operators (MNOs), this platform has expanded the range of services to include more complex services like payment of utility bills, school fees, airtime purchase, direct purchase of goods and services and now MTNMoKash. Mobile money has now made it possible for users to access their bank accounts using their mobile phones without having to physically visit their bank branches for example CenteMobile used to access bank accounts in centenary bank, This has therefore made mobile money a popular alternative to bank accounts.

For mobile money services to be widely accepted and adopted it is important for operators to overcome the following challenges, interoperability, usability, simplicity, universality, and security[1]. Among all these challenges security is the most crucial one. Currently security in mobile money platforms in Uganda rely on the use of Personal Identification Number (PIN) as an authentication method to prove if the subscriber is an authorized user for example the user initiates a service request for example cash withdraw, enters the amount he/she would wish to withdraw and then he is prompted to enter the PIN in order to complete the request. But the use of PINs as a security mechanism in such services is less effective. This is because the uniqueness aspect of the PIN is artificially set thus can easily be compromised for fraudulent purposes. Also PINs are easily misused, due to their shortcomings (Forgotten, lost, copied, shared and distributed).

This therefore calls for another layer of security in mobile money services that integrates biometric technology to make the system more secure and increase customer trust in using the service.

- Also internet subscription required a lot of money since most of the research was done online.

6.2 Recommendations

- Transactions used for demonstration are limited to balance inquiry, cash withdraw and cash deposit. However, more services offered by mobile money can also be added.
- Further development and study should be carried out in the field of integrating the application with all mobile money platforms such that the users' funds are more secure thus creating a comfortable zone for the user(s) to store large sums of money on their mobile money accounts.
- Application should be done with a server that is remote to imitate the actual Mobile money system.
- At the moment, the system is designed for a single account but for the actual mobile money system millions of customer Accounts can be handled and hosted on the MNO's servers.

6.3 Conclusion

This report explores security challenges in MMSs and weaknesses associated with the current MMA method, and the developed model that integrates biometrics authentication into the system 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 model integrated with biometrics that uses both PIN and fingerprint recognition technology has been developed as an alternative. Evaluation of the developed 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.

REFERENCES

[1] P. Chandrahas, D. Kumar, R. Karthik, T. Gonsalvis, A. Jhunjhunwala, and G. Raina, "Mobile Payment Architectures for India," in *National Conference on Communications*, 2010.

[2] S. Almuairfi, P. Veeraraghavan, and N. Chilamkurti, "IPAS: Implicit password authentication system," in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*, 2011, pp. 430-435: IEEE.

[3] S. Nanavati, M. Thieme, and R. Nanavati, "Biometrics, Identity Verification in a Networked World, Wiley Computer Publishing, 2002," ed.

[4] J. Ashbourn, *Biometrics: Advanced identity verification: the complete guide*. Springer, 2014.

[5] Y. Li and X. Xu, "Revolutionary Information System Application in Biometrics," in *Networking and Digital Society, 2009. ICNDS'09. International Conference on*, 2009, vol. 1, pp. 297-300: IEEE.

[6] F. L. Podio, "Personal authentication through biometric technologies," in *Networked Appliances, 2002. Gaithersburg. Proceedings. 2002 IEEE 4th International Workshop on*, 2002, pp. 57-66: IEEE.

[7] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology,* vol. 14, no. 1, pp. 4-20, 2004.

[8] A. Singh and K. Shahazad, "A review: secure payment system for electronic transaction," *Int J Adv Res Comput Sci Softw Eng,* vol. 2, no. 3, 2012.

[9] D. Kumar, Y. Ryu, and D. Kwon, "A survey on biometric fingerprints: The cardless payment system," in *Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on*, 2008, pp. 1-6: IEEE.

[10] V. Mauree and G. Kohli, "The Mobile Money Revolution, Part 2: Financial Inclusion Enabler," *ITU-T Technology Watch Report,* 2013.

[11] L. Gilman and M. Joyce, "Managing the Risk of Fraud in Mobile Money," *GSMA: Mobile Money for Unbanked (MMU),* 2012.

[12] C. Guo, H. J. Wang, and W. Zhu, "Smart-phone attacks and defenses," San Diego, CA.

[13] A. B. Mtaho and L. Mselle, "Securing Mobile Money Services in Tanzania: A Case of Vodacom M-Pesa," *International journal of Computer Science & Network Solutions,* vol. 2, 2014.

[14] J. L. Mudiri, "Fraud in mobile financial services," *Rapport technique, MicroSave,* p. 30, 2013.

[15] M. Belkhede, V. Gulhane, and P. Bajaj, "Biometric mechanism for enhanced security of online transaction on Android system: A design approach," in *Advanced Communication Technology (ICACT), 2012 14th International Conference on*, 2012, pp. 1193-1197: IEEE.