Global Scientific JOURNALS
GSJ: Volume 10, Issue 11, November 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

EXTENDED SECURITY MODEL FOR MOBILE MONEY EXCHANGE DELIVERY

[1]Mr NSHIMIYIMANA Modeste, [2]Dr SANJA Michael Mutongwa (PhD)

[1]Dept of Information Technology
[1]Graduate School of University of Kigali, Rwanda
[1]nmodeste2050@gmail.com

[2]Institutional Development, Research & Innovation
[2]University of Kigali Kigali , Rwanda
[2]sanja_michael@yahoo.com /msanja@uok.ac.rw

ABSTRACT

Movement of money from one person to another or from one account to another for making payment, helping families and friends is common in societies. Mobile Money, as a new financial system, is a cheaper, faster and more efficient way of carrying out financial transactions in the area, which also has an impact on Financial Security. The main objective of the study is to design the extender security model for Mobile Money exchange. The specific objectives of this study are: to examine the influence of infrastructure on mobile money exchange delivery, to inspect the influence of data flow on mobile money exchange delivery, to establish the effects of security on mobile money exchange delivery, and finally to evaluate the novel security model for mobile money exchange delivery. The target population was 250 individuals. The sample size of 153 respondents has been drawn from the target population. Data for the study have been be collected from the selected transport company and its different customers through a self-administered questionnaire. This study presented an assortment of findings start with demographic findings. A great number (54.25%) of the respondents employed in this study were female and most of them (51.63%) and most of the respondents were in middle age between 20 and 25 years of age. 26.80% of respondents were Bank teller. Furthermore, the majority of respondents (50.98%) had A2 level. The main technologies currently employed for mobile money mobile money transfers are: SMS, STK, USSD, and Wireless Application Protocol (WAP). SMS technology: SMS is that the most ordinarily used application in mobile cash transfers in developing countries for low-value payments as a result of it's easy to use and is compatible with a spread of phones as well as low-end devices. STK technology: STK is a standard from GSM which has been used since 1998 to secure mobile phone applications, especially for mobile banking and privacy. The researcher has used different network devices to design the model below. Among those tools include computers, switches, routers, file servers, web servers, as well as firewall. The researcher used a firewall for security purpose because a firewall monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. To simulate the model, researcher has used the Packet tracer 8.1.1 software to test the data flow from outside network to inside network. The mobile money exchange are understood as the services whereby customers use their mobile device to send and receive monetary value or more simply put, to transfer money electronically from one person to another using a mobile phone. The nodes from different network can communicate and packet have successfully flowed through the firewall which is configured to allow some packets and restrict others from any outside network.

Keywords: *Security; Mobile Money Exchange Delivery*

1. INTRODUCTION

Advancement in mobile money exchange technology has created new opportunities, and risks for businesses, service providers and users of these new technologies. Some individuals have adopted these new technologies to remain competitive and current with new technological developments. However, before mobile money exchange, financial transactions and services were carried out differently, and the weakness of the systems necessitated the coming of Mobile Money. Transferring money from person to person started in 1871 in USA. From there, money transfer services were introduced thereafter (Azeh, 2018). In the 1980s, in New York City, USA, online banking came into being. In the 1980s, online banking meant using a keyboard, and computer monitor to access one's bank account using a landline telephone (Bisong, 2018).

Mobile Money is loosely referred to as money stored in the Subscriber Identity Module (SIM) as an identifier rather than an account number in the conventional banking business (Azeh, 2018). Mobile Money differs from mobile banking in that, for a user to use mobile banking for financial transactions, a bank account is required whereas, Mobile Money does not necessarily need a bank account. Mobile Money uses Electronic or E-money and SMS to function.

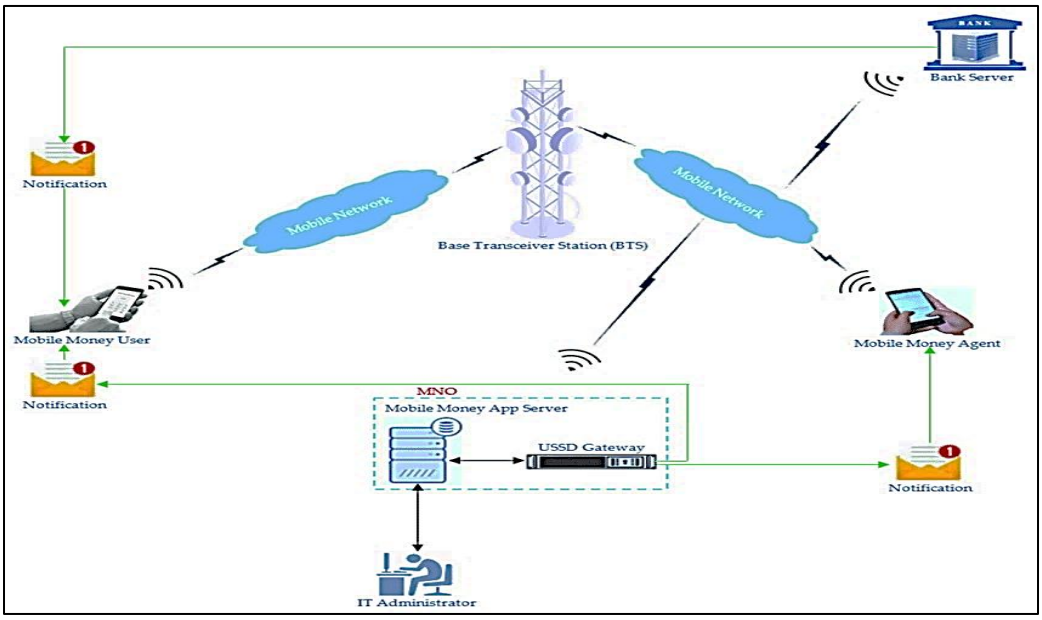

Figure 1: Mobile Money Architecure (McKinsey Global Institute, 2016)

End-to-end encryption is presently not out there. The encryption rule used is A5 that has verified to be vulnerable. SMS is not the best platform for creating payments owing to security problems, as messages travel and area unit keep on the mobile device in plain text while not encrypted. STK may be a customary from GSM that has been used since 1998 to secure transportable applications, particularly for mobile banking and privacy.

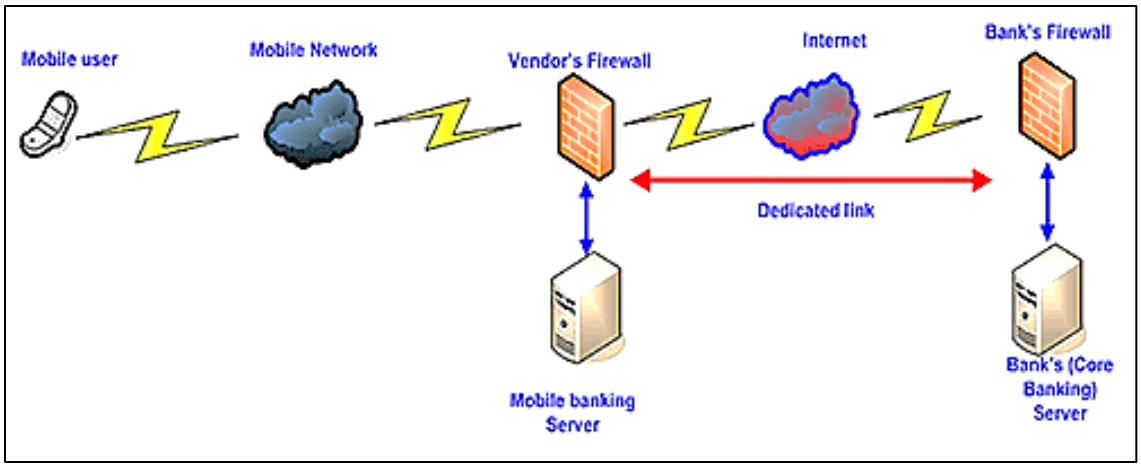

Figure 2: Mobile banking app security (Kisutsa, 2016)

The firewalling of mobile money and other business IT systems can discourage growth and add cost, thereby reducing profitability. Several countries require such a firewall to protect mobile money customers against control failures outside of the mobile money business in the voice and data business of an MNO (Mobile Network Operator).

Mobile Money is a new phenomenon that came to Rwanda in 2012, and since its coming, the number of people using the services within its short period of existence, had recorded a significant number of users, as of September 2016, the services recorded 2.7 million subscribers to MTN Mobile Money services in Rwanda (Ntambara, 2021).

2. LITERATURE REVIEW

2.1 Financial Security

Financial Security is view as a means by which people use to determine their social status in society. Hope in examining the effect of financial security on social interactions measured the effect of financial vulnerability or financial insecurity in the dimension of safety nets (Creswell, 2012), toward community involvement.

2.2 Mobile Money Security

Eric Kodjo Afanu & Raymond Selorm Mamattah in examining Mobile Money security, they examined the measures that mobile network operators providing Mobile Money services can employ to prevent fraud. The study identified that one of the major issue affecting Mobile Money security is fraud. The study brings in the idea of how secure are you using Mobile Money and identified pin sharing as one of the main issue affecting Mobile Money security. The study also studied the relationship between mobile phone protection and security of the Mobile Money service on their phone (Creswell, 2012), which were found to be closely related as the security of one can affect the other. The study examined mobile phones and how they are related to Mobile Money security.

2.3 Key Challenges in the Mobile Money Landscape

There are various challenges affecting mobile money services and digital payments which range from lack of infrastructure, awareness, digital literacy and privacy concerns; Interoperability; the interconnection between telecom operators remains a barrier to customers when sending money from one operator to another therefore payment systems must be interoperable with banks and MoMo platforms across all telecom operators. Security and privacy concerns; there have been several money fraud cases where unauthorized people try to trick people to channel their money to their MoMo accounts, this reduces trust and confidence for people using digital payments. Sustainability of operations.

2.4 Technologies used for mobile money transfers

1. SMS technology

SMS is that the most ordinarily used application in mobile cash transfers in developing countries for low-value payments as a result of it's easy to use and is compatible with a spread of phones as well as low-end devices (Bill & Melinda Gates, 2012). The default information for SMS messages is plaintext. The sole coding concerned throughout transmission is that the coding between the bottom transceiver station and the mobile station. End-to-end encryption is presently not out there. The encryption rule used is A5 that has verified to be vulnerable. SMS is not the best platform for creating payments owing to security problems, as messages travel and area unit keep on the mobile device in plain text while not encrypted.

2. STK technology

STK is a standard from GSM which has been used since 1998 to secure mobile phone applications, especially for mobile banking and privacy. A passcode or PIN is needed to access the application, which is stored on the SIM card. The keys to encrypt the session between the mobile device and the wireless gateway of the MNOs (Mobile Network Operators) are also stored on the SIM card. The data transmitted between the device and the wireless gateway is encrypted by the keys on the mobile device. At the wireless gateway the data is decrypted and encrypted again using the keys at the wireless gateway for transmission to the financial services institution gateway (Bill & Melinda Gates, 2012).

3. USSD technology

Unlike SMS, USSD is session-oriented, which has the advantage that it will inform the user whether a message has reached the recipient or not. Moreover, no session information is held on the mobile device. However, the message remains sent in plain text as in SMS. USSD may also be wont to transfer cash to the user's balance on the SIM card and to deliver only once Passwords or PIN codes.

4. WAP technology

WAP-based implementations, however, will give higher security, as knowledge square measure encrypted between the client and therefore the merchant/bank. WAP implementations square measure a lot of common with banks adding mobile as another channel for users to access their accounts.

2.5 WAP Environment

The WAP environment defines the framework for network-neutral, wireless applications for narrowband devices. WAP entree acts because the bridge between the wireless network containing wireless purchasers and therefore the electronic network containing application servers.

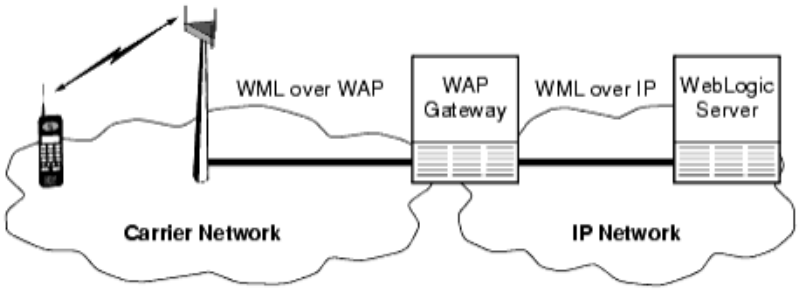

Figure 3: WAP Application Architecture

2.6 WAP Gateway Security and Security Concerns

The security layer of the WAP protocol stack is termed Wireless Transport Layer Security (WTLS). WTLS is predicated upon the established Transport-Layer Security (TLS) protocol commonplace.

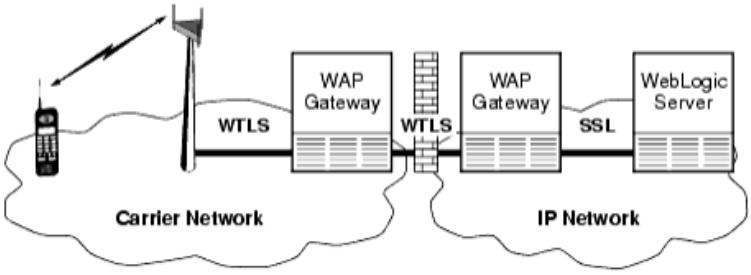

Figure 4: WAP Security Concern

For a secure connection using the WAP protocol, little security risk exists at the WAP gateway throughout the switching of WTLS (WAP side) to SSL (IP side) and SSL to WTLS. Since the WAP protocol permits a session to be redirected from the carrier's gateway to the enterprise's gateway, enterprise might want to manage this lowest risk by together with a WAP entree behind its firewall.

3. RESEARCH METHODOLOGY

Research Design; Study population; Sample size; Data collection tools

3.1 Research Design

Researcher consulted secondary data and experts publications on the subject being studied. Literature to consult was obtained from tangible and/or non-tangible media and Internet media in the form of journals, e-books and other materials relevant to security for mobile money exchange delivery to find out how to bridge the gap identified in current model.

3.2 Study population

The target population was the Liquid Intelligent Technologies employers and employees of Kigali, Rwanda. In this context, the population of this study included eBanking Officers, eBanking Agents, IT managers, Bank tellers and Operations Officer. The total population will be 250 personnel.

3.3 Sample size

The sample is done in from knowledge gained to represent the entire target under study (Cohen et al., 2011). Sampling is the action of selecting the quantity of observations to include in a statistical sample. The sample size of 153 respondents was drawn from the target population

3.4 Tools for data collection

Data collection involves gathering of data using defined techniques in order to answer the pre-determined research question of the study (Sam, 2012). Researcher used questionnaire as an instrument consisting of questions for gathering information from respondents. Researcher used questionnaire because the study concerned with variables that could not be observed such as views, opinions, perceptions, and feelings of the respondents.

4. ANALYSIS AND FINDINGS

4.1 Model design

The proposed model comprises the gateway between the web browser and a web server. WAP gateway translates all the protocols used in WAP to the protocols used on the Internet. For security purpose, the introduction of firewalls is mandatory. The mobile device and the WAP gateway communicate via WTLS. WTLS is only used between the mobile device and the WAP gateway, instead of SSL/TLS that can be used between the gateway and the Internet. This means that the WAP gateway first has to decrypt the encrypted WTLS-traffic and then has to encrypt it again (using SSL/TLS). As they pass through the firewall, the data filtering will be applied.

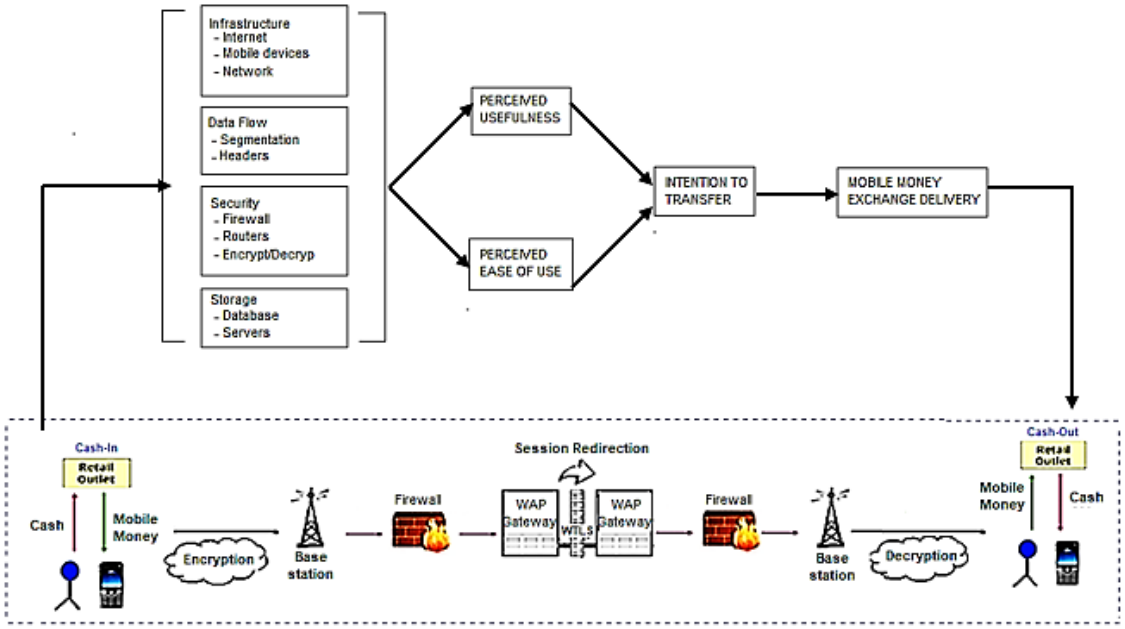

Figure 5: Proposed model (Source: Own drawing)

It utilizes the constructs perceived usefulness and perceived ease of use, which are individual beliefs that are affected by external variables. Both of these constructs, in turn, affect attitude toward using and behavioral intentional use. This model hypothesizes a relationship between external variables and both perceived usefulness and perceived ease of use (Davis, 1989).

External variables to be included are the following: Infrastructure (internet, mobile devices, network), Data Flow (segmentation, IP headers), Security (firewalls, routers, encryption and decryption), and finally the storage (database, servers). In the proposed model, before data are transmitted from sender to receiver, they have to pass encryption step to enhance their security.

4.2 New extended security model

The researcher has used different network devices to design the model below. Among those tools include computers, switches, routers, file servers, web servers, as well as firewall. The researcher used a firewall for security purpose because a firewall monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

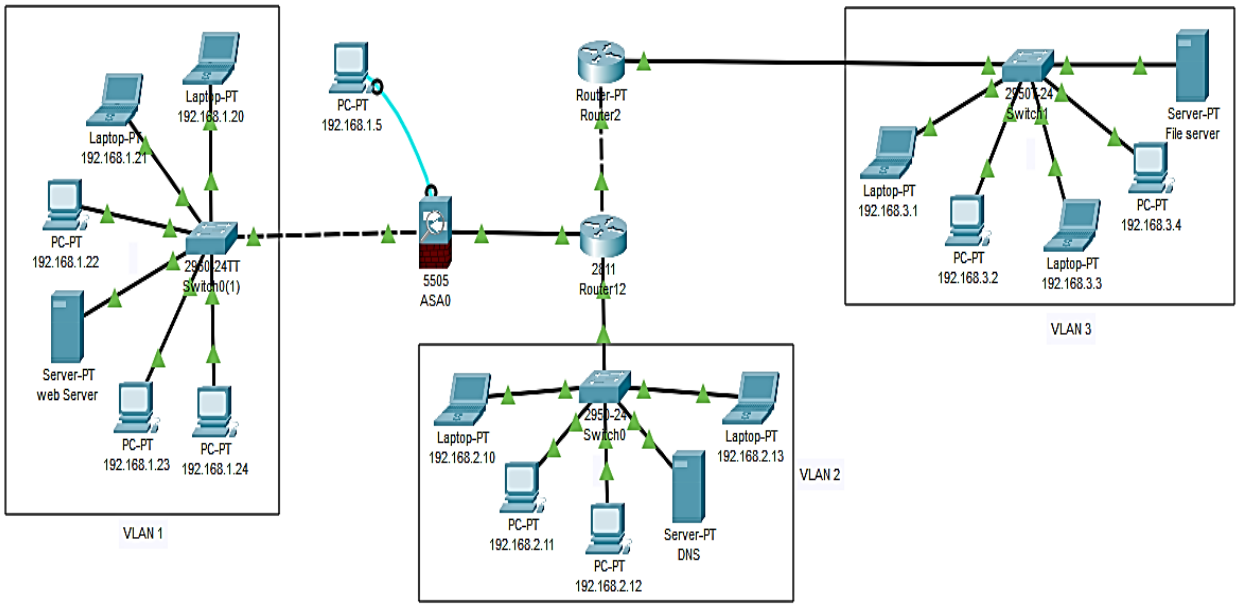

Figure 6: Model design

The network of VLAN 1 is directly connected to the firewall, thus it cannot openly communicate with other networks without passing through the firewall. In this design, the firewall plays many roles such as packet filtering, application gateway, network policy, and advanced authentication.

Packet filtering

IP packet filtering is accomplished using a packet filtering router that filters packets as they pass between the router's interfaces. A packet-filtering router usually can filter IP packets based on source IP address, destination IP address, TCP/UDP source port, or destination port.

Application gateway

To counter the weaknesses associated with packet filtering routers, firewalls need to use software applications to forward and filter connections for services such as Telnet and FTP. Such an application is referred to as a proxy service, while the host running the proxy service is referred to as an application gateway.

Network policy

The higher-level policy is an issue-specific network access policy that defines services that are allowed or explicitly denied from the restricted network, how they would be used, and the conditions for exceptions to this policy. The lower-level policy discloses how the firewall will handle access restriction and service filtration defined in the higher-level policy.

4.3 Model simulation

The model testing was made possible by the use of Packet Tracer 8.1.1 software, which is the latest version to handle such a task. The researcher has simulated a three-VLAN network by the help of firewall for information filtering as the data are flowing through the network, as shown in figure below.

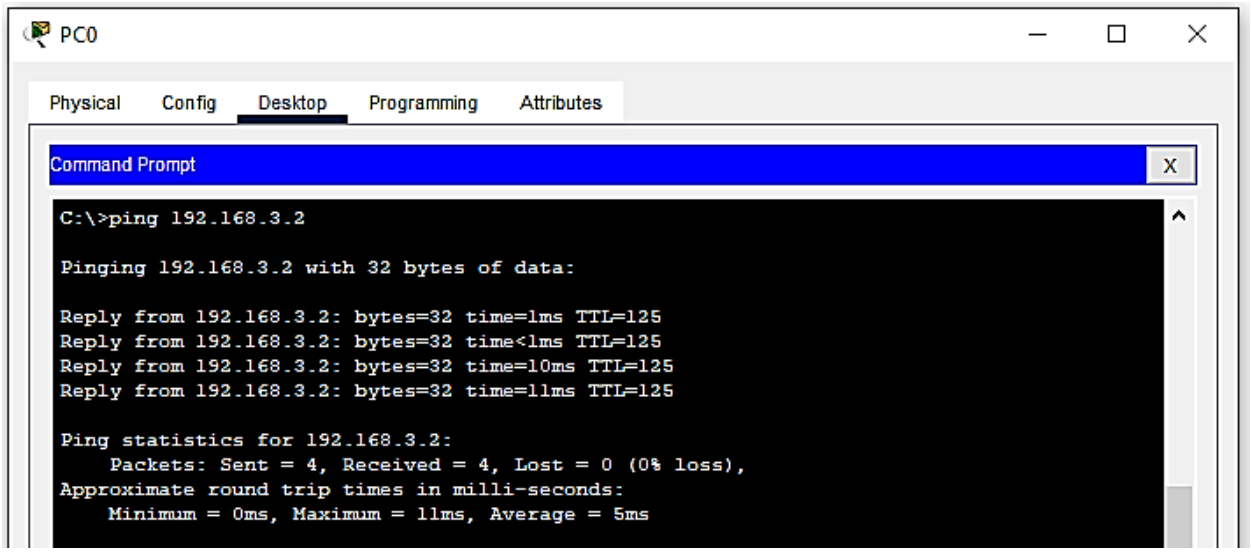

Figure 7: Ping results from PC0

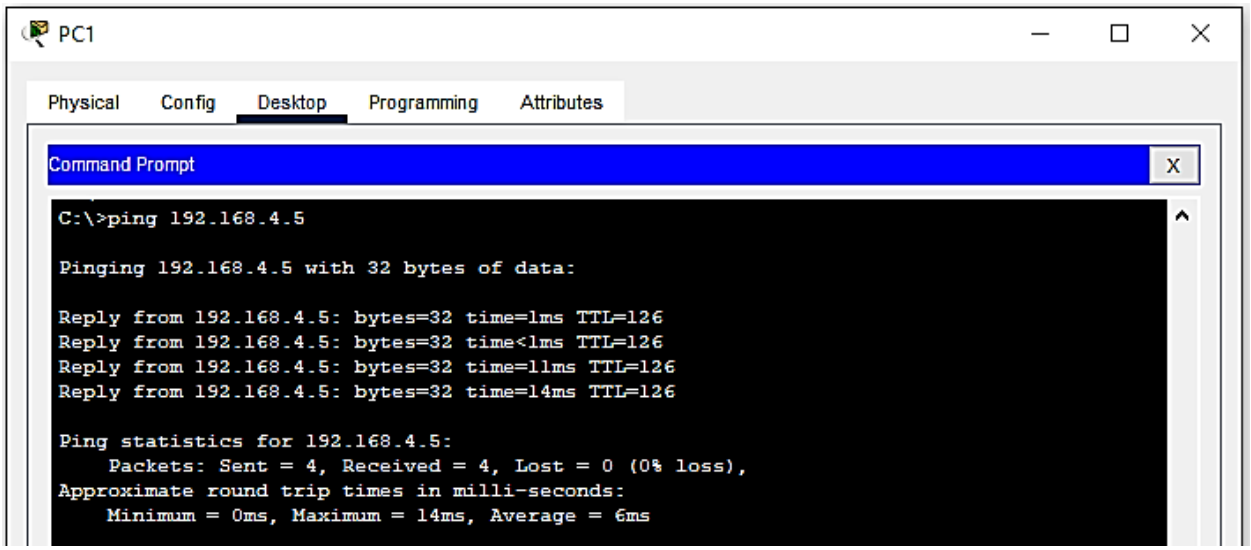

Figure 8: Ping results from PC1

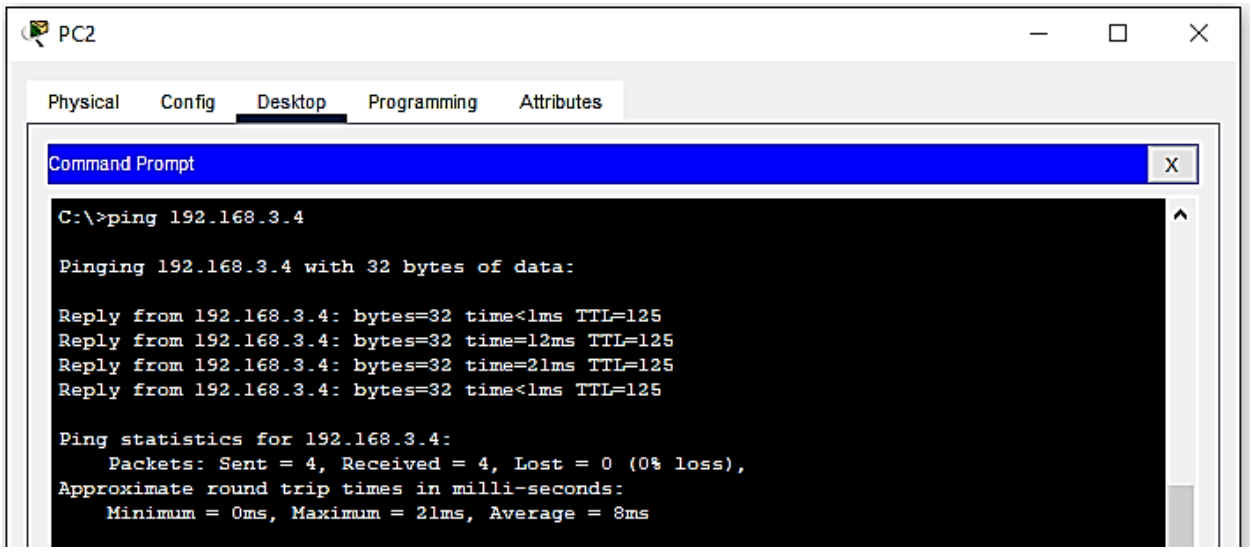

Figure 9: Ping results from PC2

To simulate the model, researcher has used the Packet tracer 8.1.1 software to test the data flow from outside network to inside network. The mobile money exchange are understood as the services whereby customers use their mobile device to send and receive monetary value or more simply put, to transfer money electronically from one person to another using a mobile phone.

During this process, both domestic transfers as well as international, or cross-border, remittances are money transfer services have been considered. The nodes from different network can communicate and packet have successfully flowed through the firewall which is configured to allow some packets and restrict others from any outside network.

5. CONCLUSION

The drive of this research was to develop an extended security model for mobile money exchange delivery. This study presented an assortment of findings start with demographic findings. The main technologies currently employed for mobile money mobile money transfers are: SMS, STK, USSD, and Wireless Application Protocol (WAP). The researcher has used different network devices to design the model below. Among those tools include computers, switches, routers, file servers, web servers, as well as firewall. The researcher used a firewall for security purpose because a firewall monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. To simulate the model, researcher has used the Packet tracer 8.1.1 software to test the data flow from outside network to inside network. The mobile money exchange are understood as the services whereby customers use their mobile device to send and receive monetary value or more simply put, to transfer money electronically from one person to another using a mobile phone. During this process, both domestic transfers as well as international, or cross-border, remittances are money transfer services have been considered. The nodes from different network can communicate and packet have successfully flowed through the firewall which is configured to allow some packets and restrict others from any outside network.

REFERENCES

[1] Azeh, Roland, Aged 29, Procument Officer ETS ANAMSE, Buea, 17 July 2018.

[2] Berg, B. L. (2000). Qualitative research methods for the social sciences. Ebook.4th ed. Boston: Allyn & Bacon.

[3] Bill and Melinda Gates Foundation / Jake Kendall: MMU Data From Advanced Mobile Money Markets. (2012), Jake Kendall.

[4] Bill Gardner. (2020, March 02). Dirty banknotes may be spreading the coronavirus, WHO suggests. The Telegraph.

[5] Bisong, Claude, age 26, businessman, Buea, July 20, 2018.

[6] BNR. (2019). BNR Annual Report 2019-2020. Kigali: National Bank of Rwanda.

[7] Creswell, J. (2012). Research design; qualitative, quantitative, and mixed methods approaches. Ebook. 2nd Ed. Sage Publications.

[8] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science, 35(8), 982–1003.

[9] Denzin, N., & Lincold, Y. (2005). The Sage Handbook of Qualitative Ressearch, *The discipline and practice of qualitative research*. Ebook. London; Sage Publications.

[10] Digital finance for all: Powering inclusive growth in emerging economies, McKinsey Global Institute, September 2016.

[11] GSMA (Global System Mobile Association). 2015. Mobile Phone Business InformationGSMA, London, England.

[12] Huyer, S. 2012. Gender Mainstreaming in ICT for Agriculture. USAID, Washington DC, Kodjo, E., Afanu, R., & Selorm, M. (2013). "Mobile Money Security –A Holistic Approach" (M.Sc diss. Luleå University of Technology.

[13] Regulatory Landscape for Mobile Banking. ITU GSR Discussion Paper, 2020.

[14] Viswanath Venkatesh, Michael G. Morris, and Gordon B. Davis, "User acceptance of information technology; towards a unified view," MIS Quarterly, vol. 27, no. 3(September 2003): 446-454