International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 9, Number 3 (June, 2020), pp.16-22

http://www.meacse.org/ijcar

Holistic Approach to Mobile Cash Transaction

Bulama Mohammed, Bala Yakubu Mohammed Abba Hassan and Mohammed Lamir Isah

Abubakar Tatari Ali Polytechnic Bauchi, School of Science & Technology, Nigeria

Abstract

African countries are exponentially using mobile money for transactions, with the potential to revolutionize Africa's dominant cashless economy. With the increase in cashless transactions via mobile devices and the number of daily dealings in businesses, it is essential to develop a comprehensive approach to mobile financial security that reduces security exposure and prevents fraud, as some providers have lost millions of dollars of mobile money to this growing threat. This investigation was a case study on Nigerian mobile financial security and collected qualitative and quantitative data through questionnaires and structured interviews with key mobile network operator (MNO) staff. The main conclusions of the research are the general notion that there is no direct link concerning mobile phone protection and mobile money security. It has also been found that one of the main causes of consumer-led fraud is PIN sharing. When dealing with mobile money fraud, we recommend that the service provider provide users with countermeasure guidelines on mobile money security every four months through short message service (SMS) to alert them to the security of their mobile phones.

***Keywords*:** Fraud; Security; Cashless; GSM; PIN.

Introduction

Mobile money involves using telecommunications platforms by users or subscribers to perform banking transactions via mobile devices. Mobile money allowed users to execute transfer funds, pay bills, check balance as well as other banking activities without going to the bank or using cash. This type of cashless transactions has grown exponentially in African countries, being positioned as the next "big thing" to revolutionize the dominant African cash economy. According to [1] there are 20 countries in which 10% of adults were using mobile money at one time in 2011, of which 15 are in African countries. For example, majority of adults in Sudan, Kenya and Gabon have used mobile money [1]. Therefore, telecommunications companies in Africa are offering mobile money transaction now with or without internet in the user's mobile device. If a user is short of data or does not have a smart device can use unstructured data supplement service (USSD) code to perform banking transactions so long as it is the number users registered in their bank. For example, Nigeria's top telecom companies - MTN, Glo and Airtel offer their customers mobile money services with or without a data in user's device, and usage statistics are growing every day.

As cashless transactions are at the increased via use of mobile money services, it is essential to study the security practices of mobile network operators as well as its subscribers to ensure security for customers, to avoid fraudulent activities. These fraudulent acts and cases leading to

loss of millions of US dollars are making the users/subscribers to lack confidence in security from their operators. In an online newspaper - [2] reports a case of mobile money fraud MTN Uganda in which company staff stole millions of dollars from mobile money users. In African countries there is inadequate awareness and study on mobile money fraudulent activities. Therefore, the accurate amount and nature of fraudulent issues are still fully definite for MNO and mobile users, while it is anticipated that the mobile money service will be really attractive to fraudsters. Mobile phone sales worldwide are estimated to be worth $ 617 billion to 448 million users by 2016 [3]. In considering this situation, given the increasing use of mobile financial services, and the use of everyday issues, it is important to design a comprehensive model of mobile financial security that will be minimized. provide safety evidence and prevent fraud. From the numerous publications reviewed, it is clear that a large number of authors consider security and privacy a critical factor in the use of mobile money for payments. However, there is no clear focus on security from the start of the trade to its completion using fast cash flow for payment purposes. Most texts emphasize the central or core areas of security such as privacy, integrity, access, authentication and authorization, with no direct link to cell phone security and security.

Related Work

A mobile payment referred to a payment that has been done via mobile device. Mobile devices can be used to initiate, authorize and declare an exchange of financial value in return for goods and services [4]. Smart mobile phones, ordinary mobile phone, tablets or any other device that has subscriber identity module (SIM) card and can connect to mobile telecommunications networks and enable payment [5]. Depending on the ways the mobile network operators (MNO) lends itself to providing the service, a subscriber may be restricted to the use of one or all of the other mobile devices mentioned above.

Majority of users think that m-money is same as e-money. There is difference between the latter. E-money consist of a wider notion that includes payments made using contact cards, near field communication (NFC), credit cards, prepaid cards, debit cards, automatic teller machines (ATMs), as well as mobile phones. However, mobile money is a section of e-money in which financial services and transactions are made using mobile devices. The said services could be or could not be directly linked to users personal account or connected to credit, prepaid, or debit cards [6]. Due to the fact that mobile devices are affordable to all and the conventional banking system is frustrating as well as time consuming, all the mobile network operators in African countries are integrating m-money in their services. In over one billion subscribers to mobile network operators in developing markets have access to a mobile phone but do not have a formal bank account [7]. Penetration of mobile devices in African countries offers the essential platform for connecting with poor people in rural areas without having a financial service.

Short messages service (SMS) is the common and most used technology used for long distance transfer. Unstructured data supplement service (USSD) technology is also user friendly and fastest way to transfer funds. Subscribers with ordinary phone or smart phones that runs out of data can use USSD anytime anywhere. These technologies are now among the Mobile Network Operators (MNOs) that provide a service. Another technology used in mobile money services is the latest version of the SIM Tools Application (STK), an application attached to the subscriber identity module (SIM) card, at the bottom. portable memory used on certain mobile phones, with good network security [6]. Majority of the service providers adopt all technological avenues to provide mobile money transfer services to their subscribers. Smartphones are rapidly spreading around the world at low cost, and their enhanced capabilities of mobile cash applications will move beyond the mobile cash channel and move to more competitive areas. Despite the high demand for smartphones and the potential for enhanced transactions, the operation of SMS and

USSD will be critical to achieving a larger customer base [7]. Payment faster than sales sites, NFC, for mobile phones or cards allows the user to pay by transmitting the phone or card to the recipient [6].

Methodology

Hybrid method was employed in this study, i.e. using both qualitative and quantitative methods. Quantitative method is measurable thus require data collection techniques, for instance questionnaire or analysis as graphs or statistics that generates numerical data. Qualitative method, alternatively is not measurable but is subjective assessment of attitudes, opinions and behavior of a phenomenon. Hence, this method usually produces results either in non-quantitative form or in the form which does not require rigorous quantitative analysis [8] [9]. The objective of using hybrid method is for better interpretation and presentation of findings.

The study is categorized as follows: questionnaire was distributed to subscribers to collect information about their views on mobile device security and revenue security. This was further reviewed in order to draw conclusions about their views on these relationships. This process was used because some of the conclusions were presented as informants of the interviewees in order to gain an understanding of the information.

The findings of the study are examining ways in which the mobile money service can be better insured to prevent fraud. This goal is achieved by examining the methods used in the case study and the practices identified by studies on the security of accelerated funds. This study is also informative, as researchers gather data and analyze data to understand and explain what investors believe is the connection between mobile and financial security. The research study selected for this paper was case study. Case study was selected in other to aid the researchers to study a phenomenon in its natural setting by using numerous data collection methods to gather information from one to many entities [11] [12] [13] [14]. Case study also aids the researchers with prospect to adopt the chosen research design i.e. exploratory and descriptive.

The locations for data collection were influenced by the nature of the data required for this study (the responses to the interview / questionnaire from mobile money users and key personnel of the case study company). Mobile money users are based in the company's service centers in Nigeria's ten regional capitals. These service centers are located in various viewpoints along the main administrative cities with easy access to subscribers. Mobile voice, data and money services are provided to subscribers by the service centers. Additionally, there are trader's shacks known as service centers for mobile money, the traders provide platforms for receiving mobile money funds or transferring funds by those who does not own mobile devices. Finding merchant stores is not easy and they have small subscriber activities and are not suitable for finding mobile money users. Service centers are usually concentrated in regional capitals. Client supervisory authorities in the service centers applied for the authorization to obtain the place of mobile money users and data collection by the research team.

Result & Discussion

53% of the total respondents are men, and 47% are women. Respondents age groups, aged between 18 and 29 years has 67% of total respondents, ages between 30 and 39 years are 26%, and ages ranging between 40 and 49 years are 7%. There is no response in the ages ranging 50-59 years or over 60 years. 34% of the respondents obtained a diploma-level education, also 33% out of the respondents are bachelor's degree graduates. Senior secondary students (SSS) as well as those with no educational background make up 21%, 7%, 5% respectively.

Period for mobile money usage

Table 1-1 below shows how long the respondents had subscribed to the mobile money service.

Table 1-1 Period for using Mobile Money

Options	Frequency
< 1 year	31
1-2 years	33
3-4 years	36
Total	**100**

Table 1-2 Desired point to load money on phone

Options	Frequency
Service centers	73
Banks	12
Merchants	14
Peer-to-peer	1
Total	**100**

The above Table 1-2 pinpoints the desired points to load money in mobile device according to respondents. The table indicates that 73 out of the respondents desire the service provider's service center to the other sources available. 12, 14 and 1 out of the respondents desired banks, merchants and peer-to-peer respectively.

Table 1-3 Desired platform to transfer money

Options	Frequency
Own phone (self)	51
Service centers	43
Merchants	6
Total	**100**

Table 1-3 denotes to subscribers for mobile money responses as the most suitable means of funds transfer. The existing means offered to the respondents are: using their mobile device to transfer funds, going to service centers or going to shacks for fund transfer. 51 out of 100 are using their mobile device to transfer funds which is the majority of the responses. Alternative

option which follows was 43 of the respondents were using service centers to transfer funds hence, 6 of respondents preferred the merchants.

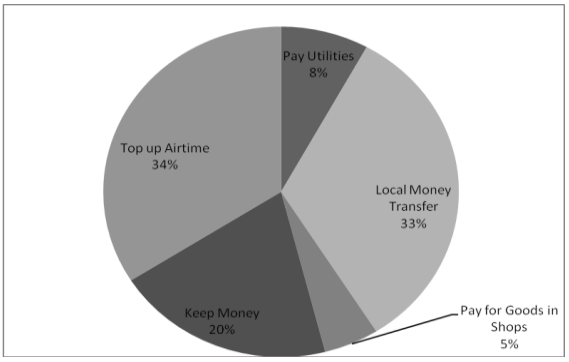

Figure 1-1 Mobile money usage

Above figure denotes the respondents' distribution in percentage for the numerous uses of mobile money. The figure displays that 34% as majority of subscribers use mobile money for air time or data replenishments, 33% preferred local money transfer. While 20% amongst the respondents use mobile money for depositing their money, whereas 8% prefer payment for utilities services and 5% use the service to pay for goods bought at shops.

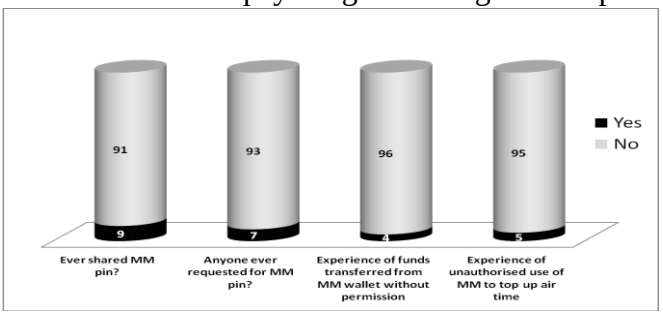

Figure 1-2 Actions susceptible to fraud

Respondents were requested to reveal whether they had ever shared their PIN for mobile money to anyone. As shown in Figure 1-2, the replies attained show that 9% of all respondents disclose their PIN for mobile money, while 91% of subscribers never disclose it to anyone. From the study, the reason why respondents cannot offer their PIN for mobile money to anyone was that they see it as confidential and could not disclose it anyone else, while others said they would not make it public to prevent fraud. Other reasons why respondents did not disclose their PIN for mobile money comprises of:

"I keep money in my mobile wallet as savings, and I can't allow my account to be ransacked"

"My security will be completely breached if I did".

In contrast, 9% of the respondents disclose their mobile money PIN to close relatives such as spouses and sisters/brothers. In some of the service centers/shacks some respondents who could not operate or transact with mobile devices confided with merchants about their PINs because they needed support.

7% of the respondents confirmed affirmative to the question 'has anyone ever requested for your mobile PIN number?', thus as seen in Fig. 1-2, 93% responded in the negative.

In Fig 1-2 above 4% of the respondents experienced automatic updates with their mobile money app without their permission i.e. experience of unauthorized transaction. 96% however responded that they had no such experience. Similarly, 95% of respondents did not used money from their mobile wallet to buy unauthorized rescue time, as contrary to the 5% who experienced it. This indicates that even though transactions in users' accounts have been executed without their knowledge, these activities are objectively minimal compared to the percentage of respondents who have had this experience. These questions were enquired in other to determine the number of respondents experienced unauthorized transactions from their mobile device

accounts. These could be the base for warning of fraud in mobile devices.

Conclusion

These studies revealed that the primary use of the mobile device services is for the purchase of top ups as well as for local fund transfers, as it is generally considered the use of mobile money in African countries. In the opinion of the researchers more people have access to mobile devices and they utilize its functionalities in banking transactions compared to conventional banking, hence mobile money popularity is in the increase. In addition, it is difficult for one to open a bank account as additional content, such as issued credentials, references from current customers and confirmation of user location is necessary. In the meantime, compared to owning a mobile account, the process is not as complex as opening a bank account. It can be further argued that people are looking for simpler and faster ways to send and receive money. It can also be argued that since mobile phone transfers are mainly made from rural cities, where most do not have a bank account, but mobile phones are accessible, it could affect their use. major carriers of mobile phones.

Since one of the main causes of consumer fraud is the distribution of PINs, this study shows that this is not a very common practice. However, 9% who shared their PINs did so through their communications and sometimes to agencies to assist them in trading one or another service with their mobile money. From this, it can be seen that PIN sharing can be based on trust, and if any fraud is protected by obtaining user PINs, the fraudster must first try to gain the user's trust or by pretending to be part of a service provider or relative who tries to help. To avoid this, scientists believe that MNOs should warn users to first verify the reliability of any suspected claims before providing information that could make them vulnerable to fraud.

References

[1] The Economist, "One business where the poorest continent is miles ahead," 2012. [Online]. Available: http://www.economist.com/node/21553510.

[2] CIO East Africa, "MTN Uganda loses over USD $3m in mobile money fraud," Online Newspaper, 2012. [Online]. Available: http://www.cio.co.ke/news/top-stories/mtnuganda-loses-over-usd-$3m-in-mobile-money-fraud.

[3] C. P. Gartner, "Mobile Payment Market Will Experience Fragmented Service Offerings in the Short Term," 2017. [Online]. Available: http://www.gartner.com/it/page.jsp?id=2028315.

[4] S. Seakomo, "Mobile phone users' information security practices, situation of students in Nigeria," LTU-EX-2012-41518700, Sweden, 2012.

[5] A. Herzberg, "Payments and banking with mobile personal devices," 2068 Communications of the ACM, vol. 46, no. 5, p. 53–58, 2003.

[6] IFC (International Finance Corporation), "Mobile Money Study," Washington, DC, 2013. [Online]. Available: http://www.ifc.org/ifcext/globalfm.nsf/Content/Mobile+Money+Study+2011 .

[7] GSMA, "“Global Mobile Money Deployment Tracker.”," GSMA Mobile Money Tracker, 2012. [Online]. Available: http://www.wirelessintelligence.com/mobile-money.

[8] World Bank, "Information and communications for development 2012: Maximizing Mobile," 2012.

[9] M. N. K. Saunders, P. Lewis and A. Thronhill, Research methods for business students, 6th ed., Pearson., 2008.

[10] S. Schwiderski-Grosche and H. Knospe, Secure M-Commerce, Information Security Group, UK: Royal Holloway University of London, Egham , 2002.

[11] I. Benbasat, "‘An analysis of research methodologies’, in The information systems research challenge, F. Warren McFarlan (ed.)," Harvard Business School Press, Boston, Massachusetts, pp. 47-85, 1984.

[12] T. V. Bonoma, "Case Research in Marketing: Opportunities, Problems, and a Process," Journal of marketing research, vol. 22, no. 2, pp. 199-208, 1985.
[13] R. S. Kaplan, "The role of empirical research in management Accounting," Division of Research, Harvard Business School, Boston, Massachusetts., no. 9-785-001, 1995.
[14] R. K. Yin, Case study research: design and methods, California: Sage Publications, Beverly Hills, 2019.