ISSN No:-2456-2165

A Framework for Addressing Mobile Money Security Vulnerabilities in Tanzania

Kenneth Longo Mlelwa
Information and Communication Technology Department
The Mwalimu Nyerere Memorial Academy
Dar es Salaam, Tanzania

Abstract:- The growth of mobile payments gave rise to several security threats to users. These threats are attributed to vulnerabilities due to ignorance, technical issues, inadequate regulations, information about mobile transactions, and lack of formal complaints and redress mechanisms. This study aimed to design a framework to address security vulnerabilities in mobile money services in Tanzania. The study was conducted at Airtel Airtel Money agents and employees in Dar es Salaam, with a sample size of 163 respondents. The results show that 77.9% of respondents said mobile money service is safe. According to the results obtained, despite the safety of mobile money services, threats and vulnerabilities were identified. Users receive calls/SMS requests to perform unintended transactions. Some users experience altering their mobile money balance, using the public internet to perform a transaction, downloading apps from the internet, and downloading data from unknown sites are the potential cause of security vulnerability and threats to mobile money services. The study recommends that mobile money operators design a safe system and raise awareness among users on security aspects. Users are to report any receipt of a call or SMS requesting them to perform an unintended transaction, and stakeholders, customers, and Government cooperate in the design and implement the safe framework for mobile money service.

Keywords:- *Vulnerabilities, Mobile Money, Threats.*

I. INTRODUCTION

Mobile Financial Services (MFS), as provided by Mobile Network Operators (MNO), are the financial services that are being provided through telecommunications registered subscribers' mobile devices. They include peer-to-peer transactions, bill payments, merchants' services for buying goods, interoperability on banks, and transfer to other mobile operators, and international remittance. Bångens and Söderberg (2008) defined Mobile financial services are financial transaction services provided by mobile network operators through mobile phones.

Mobile financial systems are also known as mobile money services or mobile money. It is a financial solution where customers or end users can perform financial transactions through mobile phones. Mobile money services are known as M-money services or SMS money services. They were started and announced in 1999, the same year Fundamo company deployed their prototype and became the world's first largest mobile financial service provider in 2002. However, the first significant deployment was made by a company called Paybox which Deutsche Bank primarily funded; Paybox company was founded by two young Germans (Mathias Entenmann and Eckart Ortwein). The solution was later deployed in other countries such as Austria, Sweden, Spain, and the UK, and in about 2003, more than a million people were registered on Paybox. Gartner rated the company as the leader in the field.

The provision of financial services by telecommunications industries without carrying cash and physically attached to different service providers has improved and eased the life of every financial institution and end-user in one way or another by serving time for other life matters and fast transactions. In the past decade, mobile money services have expanded rapidly, resulting in the financial inclusion of the low-income population that did not have access to traditional financial transaction services, as elaborated by Rwiza et al., 2020.

However, the growth of mobile payments gives rise to several security vulnerabilities and later threats to users, such as privacy violations, malware attacks, fraud, theft, deviations in the quality of services, and financial and device losses (Ali, Dida, Sam, 2020). These threats are attributed to vulnerabilities in ignorance, technical issues, inadequate regulations, inadequate information about mobile transactions, and a lack of formal complaints and redress mechanisms.

To tackle these threats, we must find the vulnerabilities causing them and realize the framework to better manage the risks before landing on the market. Rwiza, Kissaka, and Kapis (2020) developed a methodology for evaluating security threats in the MNO financial service model. They further nailed that; the security evaluation of the MNO financial service model is still in the infancy stages in developing countries. They further said that there are security vulnerabilities in the MNO financial service model in such a way that financial regulators may fail to track the creation of mobile money in the country.

II. LITERATURE REVIEW

Bassole et al. (2020) conducted a study on financial applications vulnerabilities aimed at performing vulnerability assessments, facilitating an informed assessment of the information security and privacy risks that mobile money services and payment applications face in African countries,

and creating awareness in the research and practice communities.

Broad penetrations of mobile phone usage and the availability of more powerful mobile handsets and network bandwidth have made mobile devices an attractive candidate for value-added services. Today mobile users can carry out essential money services and financial transactions such as transferring money, checking balances or paying a bill or statement, traditional money services payments, and Government bills payments, merchant's payments. On the other hand, payments are the exchange of money, either Electronic Money (e-money) or physical cash, between mutually understanding parties. For electronic payment, mobile payment is mainly used to explain and carry the meaning of these phenomena.

A study by the international firm Deloitte revealed that 660 million Africans would be equipped with smartphones in 2020, against 336 million in 2016. This high penetration rate of smartphones in African countries will increase the development and use of mobile applications, including applications related to financial transactions (Bassole et al., 2020).

Organizations are increasingly adopting mobile money services and payments as a new way of business in the 21st century. Thus, mobile money services and payment security concerns are becoming more and more pressing as phone penetration, and its associated bulk of malicious apps are increasing in developing countries. Security issues in mobile money services and payments procedure have already been discussed in the literature.

Mobile computing devices (i.e., laptops, tablets, and smartphones) can cause serious harm to organizations and device owners, their friends, and families because mobile devices are far less secure. According to Wlosinski (2016), the Verizon 2015 Data Breach Investigations Report1 states that there are tens of millions of mobile devices which, due to little processing power capacity comparable to other server-side devices, are less secure. It imposes security vulnerability and hence a threat to applications and financial services.

Positive Technologies (2020) summarizes client- and server-side vulnerabilities in mobile money services applications related to faults in application code, client-server interaction, and implementation of security mechanisms. Their report did not consider other common security weaknesses, such as failure to manage software updates.

According to Bassole et al. (2020), Android has approximately one hundred and thirty (130) permissions, including permissions that are at risk concerning their access to sensitive and personal information. Also, we can see that attackers focus on vulnerable technologies they can leverage to make quick and easy money. Hackers could target these mobile payment apps. How do we keep our-self and our money safe while also being able to take advantage of the convenience of mobile payment apps?

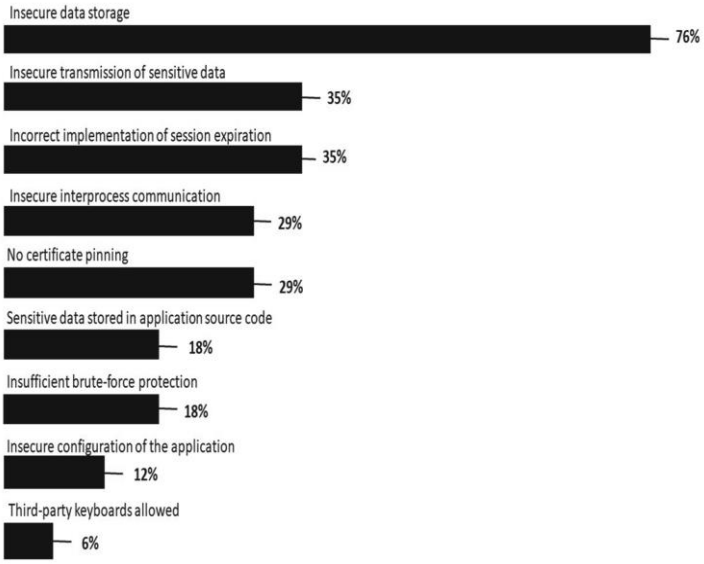

Fig. 1. Vulnerabilities of mobile applications (Source Bassole et al.)

A. Security issues in mobile money services

B. Vulnerabilities on the client side

The client-side refers to a mobile money services application installed on the user's device. There are several interfaces, in this case, client-side applications which users can use to access mobile financial services. These include mobile applications, web browsers, SIM tool Kits (STK), Interactive Voice Recorders (IVR), and Unstructured Supplementary Service Data (USSD).

These interfaces pose vulnerabilities and threats to mobile payment services from how the functionality is made. While IVR and USSD use plain text to transfer information from the subscriber handset to the server, mobile applications and web browsers use the standard HTTP(s) to exchange transactional statements.

Mobile computing device vulnerabilities exist in the device, the wireless connection, a user's practices, the organization's infrastructure, and wireless peripherals (e.g., printers, keyboard, mouse), which contain software, an OS, and a data storage device.

C. USSD, STK, and IVR vulnerabilities

USSD is Insecure communication as an attacker can tamper with USSD command requests and responses by conducting man-in-the-middle attacks using fake base stations. They can also force the phone to connect using Second Generation(2G) or Third Generation (3G), which are easier to decrypt the traffic and tamper it.

Martins (2020) explained that signaling attacks in USSD are a threat as attackers can conduct attacks by sending spoofed requests from the roaming interfaces or even target SIM Cards with vulnerable SIM Tool Kit. If the attackers send a well-crafted binary SMS with instructions to send a USSD command, the phone can send a USSD request from the victim's device, and the request will appear to be legitimate, and the mobile money solution will process it.

USSD requests are insecure in terms of authentication. It happens when authentication controls and protocols are bypassed due to poor implementation or absence. For example, weak pins leave the USSD-based menu vulnerable to brute-forcing and guessing attacks. Suppose the USSD menu for user authentication is not masked. In that case, an attacker can view the end user's credentials by conducting social engineering attacks such as shoulder surfing, which makes authentication vulnerable and becomes a threat to financial services.

Improper data validation in the USSD can lead to injection attacks that leak sensitive information. An attacker may insert specifically crafted text in the user input to perform malicious actions in the back-end server.

Broken access control occurs due to the lack of appropriate access control and allows the user to access unauthorized resources, such as features and information.

Using technology with publicly known vulnerabilities, such as the SIM-Jacker, can pose a significant security threat to the apps running on the SIM Tool Kit (STK). Using binary SMS, attackers can force the device to send malicious requests to the home network. The main Simjacker attack involves an SMS containing a specific type of spyware-like code sent to a mobile phone, which then instructs the SIM Card within the phone to 'take over the mobile phone to retrieve and perform sensitive commands (Tutorials point, 2022).

There needs to be more logging and monitoring in conjunction with a non-existent or insufficient incident response to allow fraudulent transactions to occur. More information will be available for further investigation or even stopping the ongoing attacks.

Vulnerability due to security misconfiguration occurs due to a lack of alignment between system administrators, security administrators, and other non-technical staff. Common examples of incorrect settings are Weak passwords/PINs or standard credentials that are easily guessed or poor error handling and response.

D. Mobile applications vulnerabilities

Insufficient code protection leaves MFS vulnerable to source code analysis. To exploit vulnerabilities in code, all attackers need is to download the application from Google Play or the App Store and then de-compile it. Alternatively, an attacker can use the default USSD application built into the phone.

Deep linking is a technology that allows users to navigate between applications (or sections within an application) to a specific location using special links, like hyperlinks in web applications (Lynch, Stewart, 2020). Insecure deep-link handling is a critical vulnerability that can cause financial losses for banks. For example, one money services application failed to filter deep linking URLs. Attackers could take advantage of this by loading a link to a web page containing malicious code and interacting with the JavaScript interfaces available in those components.

Obfuscation is to make it difficult for attackers to read and analyze code. Code obfuscation is a protective mechanism to reduce the attack activities on a software system (Sebastian et al., 2016). Obfuscation (Data masks) can be complete (concealing all of the original data characters) or partial (obscuring only some of the data characters). One example of code obfuscation is to remove file name characters at compile time. Random or single-letter names replace the names of classes and methods in the source. Lack of obfuscation allows attackers to analyze the code and find important data, such as Testing-related usernames and passwords, Encryption keys and parameters from which keys can be derived, and Salts for hashing and encryption.

Attackers can then use this information to obtain credentials and access web servers. Moreover, hackers can analyze the application algorithm and exploit flaws in business logic. Competitors may also want to know how the application is designed to copy new product features.

Storing sensitive information in the device is another vulnerability that can lead to threats, including taking screenshots of sensitive information and storing cached information in the device and clients to store information like passwords, money services information, and others. It must be encrypted if it is necessary to store sensitive data in the client-side device. The lack of powerful encryption in the devices is a significant leaves loophole in the security of the primary services, including MFS.

Other vulnerable components of the mobile computing device environment are the loaded apps. Each application can contain a vulnerability that is susceptible to exploitation. The apps on the mobile device can have a variety of vulnerabilities, including:

Incorrect permission settings that allow access to controlled functionality such as the camera or GPS, Exposed internal communications protocols that pass messages internally within the device to itself or to other applications, Potentially dangerous functionality that accesses the resources or the user's personal information via internal program data calls or hard-coded instructions, Application collusion, where two or more applications pass information to each other to increase the capabilities of one or both applications, obfuscation, where functionality or processing capabilities are hidden or obscured from the user, Excessive power consumption of applications running continuously in the background, which drain the battery, thereby reducing system availability, traditional software vulnerabilities such as insufficient editing of data entered, Structured Query Language (SQL) query exploitation and poor programming practices and privacy weaknesses in configuration settings that allow access to the application's sensitive information (e.g., contacts, calendar information, user tasks, personal reminders, photographs, Bluetooth access)

ISSN No:-2456-2165

Below is the distribution of vulnerabilities by type of activity the end user can use (source Positive technologies 2020).

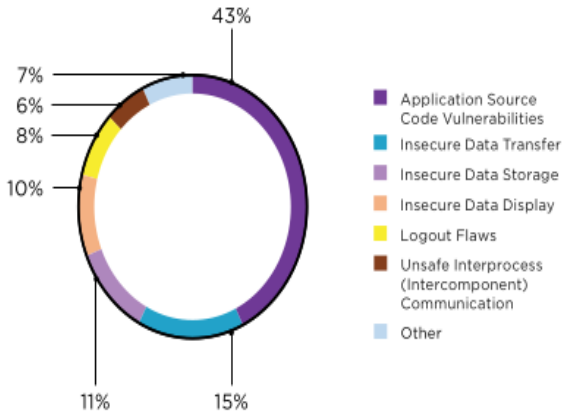

Fig. 2. Vulnerability by type (source Positive technologies 2020).

III. METHODOLOY

This study employed the mixed design of both qualitative and quantitative. The study used a quantitative approach in identifying and examining the vulnerabilities and proposing its framework for Mobile Money services. The approach was used because the study aimed at determining the relationship between security vulnerabilities [independent variables] and the framework to be designed (a dependent or outcome variable). Some features of quantitative research have been adopted to complement descriptive research. A qualitative approach was used to analyze and process secondary data.

A. Sampling, data collection and data processing

The sample design was done before the data collection. Kothari (2004) defines sample design as a definite plan for obtaining a sample from a given population. It refers to the technique or procedure the researcher would adopt to select sample items. This involves the identification of the target population, determining the size of the sample, and choosing a sampling method used for data collection based on the adopted research design.

Data processing was done to prepare collected raw data for smooth analysis. Data processing includes data cleaning, data coding, and reverse coding. Data cleaning was done by examining the collected data to identify omissions and errors and find a way to rectify them where possible. This process also checked if the returned questionnaires' data contained therein are accurate and consistent with other facts gathered, uniformly entered, and well arranged to facilitate coding and data analysis. Secondly, data coding was processed by assigning numerals or other symbols to classes into which responses were placed.

IV. RESULTS

It was revealed that 77.9% of respondents) believe that mobile money is safe. The rest believe otherwise, and this is because mobile money is vulnerable to some threats and attacks.

Some actions make MM service to be vulnerable. These include downloading the mobile APP, downloading data from the internet, receiving the wrong confirmation MM message related to the transaction, and not confirming the recipient details before the transaction.

Nowadays, mobile money users have been experiencing receipt of calls or messages asking them to perform unintended mobile money transactions. Furthermore, most of the respondents in this study experienced such a thing.

The study further discovered that there are threats identified mainly by the respondents as they highly affect the use of MM services. These threats are in Table 2, Table 3, and Figure 4.4. It was revealed that downloading data from the internet, use of public wireless internet, and mobile app misbehavior are the biggest threats to MMT. Users should avoid using the public internet when performing mobile money transactions, which may lead to security attacks. The study found that there is a possibility for mobile money balances to be altered. Thus, users should refrain from using the public internet to transact.

A dangerous threat examined and found to exist is that mobile money transactions can be exposed to the internet without the user's concern. This is shown in Table 2 that 14% of respondents agree with this threat. The respondents found that their mobile money transactions were exposed with no concerns. A few respondents have mentioned such a case, but on the other hand, most of the respondents said they did not find such an experience.

TABLE I. THREATS CAUSED BY THE SECURITY VULNERABILITY

Downloading data from the internet can be a severe problem for MM trans	**Frequency**	**(%)**	**Valid %**
No	56	34.4	34.4
Not sure	36	22.1	22.1
Yes	71	43.6	43.6

Source: Field data, 2022

ISSN No:-2456-2165

Table II shows that 82.2% of respondents did not find their MM transaction exposed anywhere.

TABLE II. OTHER MOBILE MONEY THREATS CAUSED BY THE SECURITY VULNERABILITY

MM balance can be altered		**Frequency**	**(%)**	**Valid %**
No		65	39.9	39.9
Not sure		31	19.0	19.0
Yes		67	41.1	41.1
MMT fails due to application misbehavior		**Frequency**	**(%)**	**Valid %**
No		33	20.2	20.2
Not sure		17	10.4	10.4
Yes		113	69.3	69.3
MMT is exposed to the internet or anywhere without your concerns		**Frequency**	**(%)**	**Valid %**
No		134	82.2	82.2
Not sure		6	3.7	3.7
Yes		23	14.1	14.1

Source: Field data, 2022

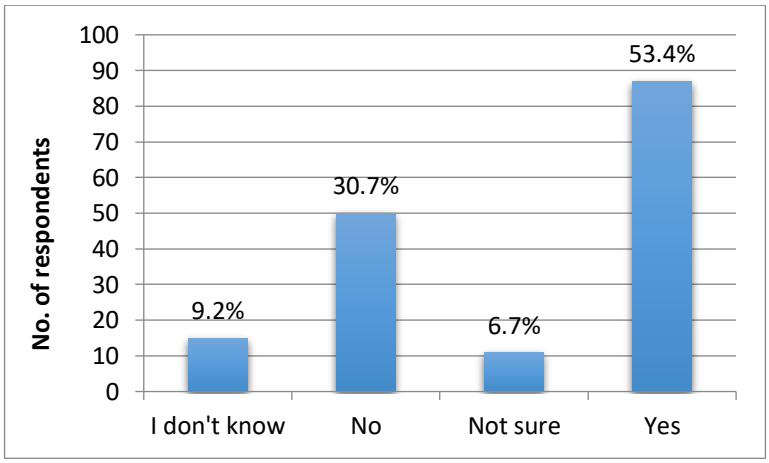

Fig. 3. Responses to the question; is Public internet risk to the mobile transaction?

A. Mobile Money framework to address a security vulnerability

The study believes that mobile money should be designed in a way that privacy will be highly maintained. The study found that those respondents with confidence in using mobile money transactions agree that there is privacy in using mobile money services. The results in Table 4 show that of respondents who have seen MMT as the safe platform, 71.6% of them said that MM services have privacy. Moreover, Table 5 shows that 55.8% of respondents said "yes" to privacy in using mobile money services.

TABLE III. CROSS-TAB FOR MMT SAFE* THERE IS PRIVACY IN MM SERVICES

		MM Services are private.			**Total**
		No	Not Sure	Yes	
MMT Safe	No	21(58.3%)	11(30.6%)	4 (11.1%)	36(22.1%)
	Yes	21(16.5%)	15(11.8%)	91(71.6%)	127(77.9%)
Total		42	26	95	163(100%)

Source: Field data, 2022

The study revealed that mobile money services should be safe and ensure the privacy of the users' transactions. The study further revealed that the users need to confirm the recipient details before initialing the transaction. The results show that several people must confirm the recipient detail before initiating the transaction. Table 5 shows that 14.1% of respondents must confirm the recipient details. However, a large number of the respondents (81.6%) do confirm the recipient details.

TABLE IV. FRAMEWORK TO ADDRESS SECURITY VULNERABILITIES

Framework		Frequency	(%)	Valid %
privacy to your mobile money services				
No		42	25.8	25.8
Not sure		30	18.4	18.4
Yes		91	55.8	55.8
Usually, confirm the recipient before initiating MM trans.				
No		23	14.1	14.1
Not sure		7	4.3	4.3
Yes		133	81.6	81.6

Source: Field data, 2022

The study also examined the ways to be used to protect mobile money service users. The study found that, among other things, there should be the responsiveness of all stakeholders. There should be responsiveness between customers and all stakeholders in the mobile money, awareness between customers and all stakeholders in the mobile money, awareness of all stakeholders, and awareness between customers and all stakeholders in the mobile money.

These ways could make a framework to address the vulnerabilities and helps mobile money transaction services users. The results in Table 6 show that 36.8% of respondents said that all stakeholders should be responsive and shared responsiveness between customers and all stakeholders in mobile money. Furthermore, 33.2% of respondents said there should be aware of all stakeholders and shared awareness between customers and all stakeholders in the mobile money services.

TABLE V. WAYS TO PROTECT MOBILE MONEY SERVICES.

Means		Frequency	(%)	Valid %
Any other:		5	3.1	3.1
Awareness of all stakeholders		13	8.0	8.0
Awareness of all stakeholders; The Government's awareness		2	1.2	1.2
Awareness of all stakeholders; The government awareness; Shared awareness between customers and all stakeholders in the mobile money		8	4.9	4.9
Awareness of all stakeholders; The government awareness; Shared awareness between customers and all stakeholders in the mobile money; Any other:		5	3.1	3.1
Customer awareness		9	5.5	5.5
Customer responsiveness		11	6.7	6.7
Responsiveness of all stakeholders		25	15.3	15.3
Shared awareness between customers and all stakeholders in the mobile money		41	25.2	25.2
Shared responsiveness between customers and all stakeholders in the mobile money		35	21.5	21.5
The government awareness		7	4.3	4.3
The government awareness; Shared awareness between customers and all stakeholders in the mobile money		1	.6	.6
The government responsiveness		1	.6	.6

Source: Field data, 2022

B. Framework to address Vulnerabilities.

In mobile money services, one must be exposed when performing mobile money transactions. Mobile money transaction exposure is a state of not having protection on performing a financial transaction. Depending on the weight of the exposure, vulnerabilities can be formed. From the study, these exposures can relate to receiving a message or a call to perform an unintended transaction that is coming randomly. This can also be contributed by performing a transaction using the public internet or performing a transaction in public as this lets hackers, shoulder surfing, see the details of the transactions.

From exposure, analysis is done, which can be done by the customer, company, or Government regarding the kind of exposure. Customer needs awareness which, with the current technology, can be obtained easily. This awareness includes security, vulnerabilities, and impacts of the threats or risks. Service providers also need awareness of the business loss, financial losses, and government penalties they may incur if a loss is caused by vulnerabilities in the company. This includes service or application misconfigurations and service settings ignorance which might result in mobile money services losses, which may lead to brand ruining. Government regulators must be aware of all the losses which customers and companies might incur, which may lead to revenue loss and customer disturbances.

Threat analysis can be handled to find how much the impact will be, which might lead to mitigation, coping, or loss, and how they can be avoided to improve mobile money security. Vulnerability solution options can be looked upon in trying to eliminate the vulnerability or reduce an impact. A preventive solution begins with an appraisal of the potential threat, which then triggers preventive actions to mitigate or prevent undesirable consequences. This process is referred to as the coping appraisal process (Monda, 2020). Mitigation would happen if the used option gave a positive solution concerning time. If an option provided is wrong or partial, the impact will increase the threat of mobile financial loss to customers, service providers, and the Government. However, sometimes the option can be neutral due to experience and existing exposure environment, which can lead to coping or resilience. This means that a customer can recover effectively from loss if the impact is not significant and the vulnerability is dealt with externally.

All three aspects (exposure, potential vulnerability analysis, and threat analysis) of the framework can be done on a mobile money environment to assist customers, service providers, and Government as a regulator to meet harmony in the mobile financial services sector. This can only be achieved by involving all stakeholders collaborating, to which 65% of all respondents agreed. The Vulnerability assessment approach (identification, analysis, and controlling) can be followed in this framework shown in Figure 4.5, in which 50.9% of respondents agreed on that.

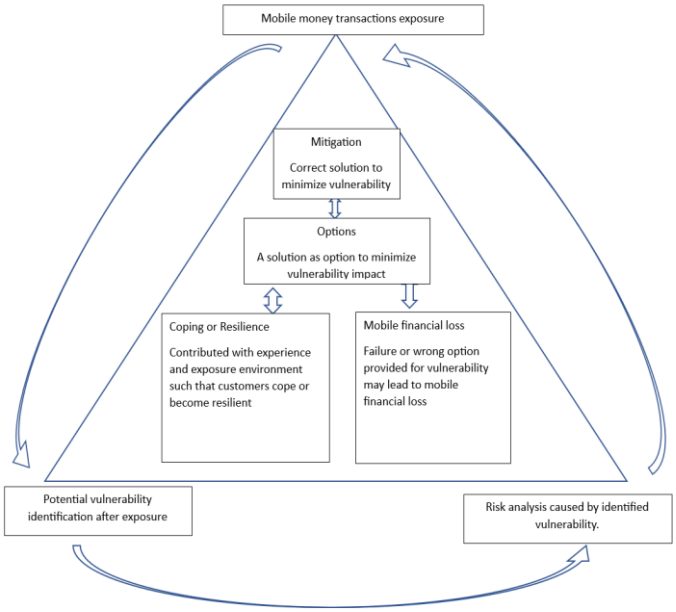

Fig. 4. Framework design

V. CONCLUSIONS AND RECOMMENDATIONS

The study aimed to design a framework to address security vulnerabilities in mobile money in Tanzania. Mobile money service in Tanzania is safe, as chapter four findings show. However, the study realized the presence of security vulnerability and threats to mobile money. Security is the major component of digital financial services, specifically Mobile Money services. Therefore, the security aspect of mobile money services is an essential concern for the successful operation of MM services.

In this study, there is an indication that the mobile money service is safe in Tanzania. Most of the respondents (77.9%) said so.

The security vulnerabilities and threats identified by the study are; downloading the mobile APP, downloading data from the internet, receiving wrong confirmation mobile money message related to the transaction, not confirming the recipient details before the transaction, receiving a call or message asking MM user to perform unintended mobile money transaction and use of public wireless internet and mobile apps misbehavior.

RECOMMENDATIONS

First, the study recommends that mobile money users choose safe approaches to using the mobile money service. They should avoid situations that may risk the transaction made by mobile money, such as avoiding using the same password for a long time, avoiding performing the transaction openly/in public, and not showing the password of mobile money. This will help them to remain safe when using mobile money services.

Secondly, mobile money operators such as Mpesa, Tigo Pesa, Airtel Money, HaloPesa, and the like should implement a safe environment for mobile money users.

Thirdly, mobile money users should report any security vulnerability or threat to the authority. For instance, when a call or SMS asking the users to perform an unintended transaction is received, users should immediately report it to the authorities and regulations. The study also recommends to the users that confirming the recipient or service name details is mandatory as it will avoid the threat and risk of theft.

Fourthly, the study recommends that stakeholders, customers, and Government cooperate in the design and implement the safe framework for mobile money service. Also, the awareness between customers, stakeholders, and shared awareness between customers and all stakeholders in mobile money should be considered.

Lastly, the study recommends that further studies be carried out to prevent security vulnerabilities and threats to mobile money services. It should also focus on different types of users, including regular citizens, not just employees and mobile money agents.

REFERENCES

[1]. Bångens, S. (2008). "Mobile money services –Financial Services for the Unbanked?" Swedish Program for ICT in Developing Regions, SPIDER [Online] URL: https://spidercenter.org/wp-content/blogs.dir/362/files/2016/11/Spider-ICT4D-Series-2-Mobile-money services-financial-services-for-the-unbanked.pdf [Accessed on]: 18/11/2021

[2]. Bassolé et al., (2020) "Vulnerability Analysis in Mobile money services and Payment Applications on Android in African Countries" ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2020 Published by Springer Nature Switzerland AG 2020. All Rights Reserved J. P. R. Thorn et al. (Eds.): Interpol 2020, LNICST 321, pp. 164–175, 2020. URL: https://doi.org/10.1007/978-3-030-51051-0_12.
[3]. Dhillon, (2007). "Principles of Information Systems Security: Text and Cases ."John Wiley & Sons Inc.
[4]. Didier, Gouayon, Yaya and Oumrouu 2020, "Vulnerability Analysis in Mobile money services and Payment Applications on Android in African Countries," [Online] [Accessed URL]: https://doi.org/10.1007/978-3-030-51051-0_12, [accessed on] 15/03/2022.
[5]. Jiow, Mwagwabi, and Low-Lim (2021). Effectiveness of protection motivation theory based: Password hygiene training program for youth media literacy education. Journal of Media Literacy Education, 13(1), 67-78. https://doi.org/10.23860/JMLE-2021-13-1-6.
[6]. Kabir (2016) "Introduction to research" [Online] [accessed URL]: https://www.researchgate.net/publication/325846733_INTRODUCTION_TO_RESEARCH [access on]: 18/11/2021.
[7]. Lynch, S. (2020). "Deep Links." [online],[Accessed URL] DOI://10.1007/978-1-4842-6700-4_6 [accessed on] 26/03/2022 .
[8]. Martin, (2020). "Mobile Security" [Online] [accessed URL]: https://medium.com/josue-martins/ussd-top-10-security-risk-for-mobile-payments-bcd64d0a34dc, [accessed on] 29/03/2022.
[9]. Mazhar and others, (2014) "An Investigation of Factors Affecting Usage and Adoption of Internet & Mobile money services In Pakistan" International Journal of Accounting and Financial Reporting (2014), V4(2).
[10]. Momani, A. (2020). The Unified Theory of Acceptance and Use of Technology: A New Approach in Technology Acceptance. International Journal of Sociotechnology and Knowledge Development. 12. 79–98. 10.4018/IJSKD.2020070105.
[11]. Nayak, Nath and Goel, (2014). "A study of adoption Behavior of Mobile money services by Indian Consumers ."International journal of research in Engineering & Technology.2(3). March 2014. 209-222.
[12]. Marathon, (2006). Fighting poverty from the street. A Survey of Street Food Vendors in Bangkok.
[13]. NTIGWIGWA(2019). Factors that Contribute to Cybercrime in Mobile Money Services in Tanzania: A Case of Kibaha Town (Doctoral dissertation, Mzumbe University).
[14]. Nyamtiga, S., Laizer (2013) "Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions" INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 1, ISSUE 3 ISSN 2347-4289.
[15]. Positive Technologies, (2020). "Vulnerabilities and threats in mobile banks" [Online] [accessed URL]: https://www.ptsecurity.com/ww-en/solutions/financial/, accessed on 16/Mar/2022.
[16]. Rumanyika, (2015). "Obstacles towards adoption of mobile money services in Tanzania: a review" International Journal of Information Technology and Business Management, v35(1) [Online]URL:http://dspace.cbe.ac.tz:8080/xmlui/bitstream/handle/123456789/269/1%20rumaniyaka%20.pdf?sequence=1&isAllowed=y [accessed on]: 18 November 2021.
[17]. Rwiza, K., Kapis, (2020). "A Methodology for Evaluating Security in MNO Financial Service Model," 2020 IST-Africa Conference (IST-Africa).
[18]. Sebastian and others, (2016). "A Study & Review on Code Obfuscation." [Online] [access URL] DOI: 10.1109/STARTUP.2016.7583913 [Accessed on] 27/03/2022.
[19]. Tutorialspoint, (2022). "What is a Simjacker attack?" [Online] [accessed URL] https://www.tutorialspoint.com/what-is-simjacker attack#:~:text=At%20its%20most%20basic%20level,receive%20and%20conduct%20sensitive%20orders. [Accessed on] 29/03/2022.
[20]. Wlosinski, (2016). "Mobile Computing Device Threats, Vulnerabilities and Risk Are Ubiquitous," ISACA JOURNAL, [online] [Accessed URL]: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/mobile-computing-device-threats-vulnerabilities-and-risk-are-ubiquitous, [accessed on] 15/03/2022.
[21]. Wodo, S., Błaśkiewicz (2021) "Security issues of electronic and mobile money services" Conference: 18th International Conference on Security and Cryptography: SECRYPT 2021 [Online]: DOI:10.5220/0010466606310638 (accessed on) 14/06/2022.