International Journal of Information and Communication Technology Research

http://www.esjournals.org

Mobile phone based payment authentication system: An intervention for customers' bank account fraud in Tanzania

Edvin J. Kitindi[1], Alcardo Alex[1], Camilius Sanga[1], Ayubu Shabani[1], George Kibirige[1], Joseph Phillip[1], Julius Oketchi[2]

[1]Sokoine University of Agriculture, P.O Box 3000, Morogoro Tanzania
[2]Masinde Muliro University of Science and Technology, Kenya

ABSTRACT

Through the rapid development of ICTs in Tanzania, banking industry has experienced rapid change in the ways of service delivery to their customers. The society has experienced a rapid development in communication sector particularly on the use of mobile phones for banking. The commercial banks in Tanzania have also revolved their ways of operating and serving their customers. The central bank of Tanzania (BoT) is responsible in defining all the payment systems in Tanzania and control all the transaction being done by the commercial banks operating in the land of Tanzania. Currently, Tanzania has many payment instruments as defined by the BoT which divided into two main group Cash and Non-Cash payments instruments. The latter includes: payment orders, bills of exchange, promissory notes, cheques and the electronic payment systems. In this paper, the security threats of these payment instruments have been discussed in detail. Some reported cases where organizations have been fleeced of their financial resources through dubious activities in Tanzania have been reviewed to verify the existing of the problem in discussion. In this paper, a Mobile phone based payment authentication system model to reduce the threats associated with non-cash payment implemented in Tanzania is proposed. Using this model, account holders are required to provide a final authentication of transaction through their registered mobile phone. This method if adopted will take care for any non-cash payment instruments. Also, some of the threats being discussed in this paper can be addressed by the proposed model.

Keywords: *Mobile phone, Payment instruments, Bank account security, Customer, Bank account, Signatory, authentication.*

1. INTRODUCTION

With the wide expansion of information and communication technologies (ICTs) into the business world, business organizations have changed the way of delivering services to their customers [1]. It has been revealed in Tanzania where there is a rapid growth of ICTs infrastructures, the banking industry also has responded positively in terms of service delivery to their customers. The use of mobile phone for example makes easy for the customer to check their balances; pay some bills and money transfer from their account to other accounts hence, mobile phone becomes key ingredient in banking operations.

Mobile phones have become an integral part of the 21st century landscape with penetration of 4.5 billion by 2011 [2]. While North America and Europe have the highest penetration rates, reaching 100% in many Western countries, South America and Asia represent the fastest growing mobile markets [3]. In developing countries, the role of the mobile phone is more extensive than in developed countries, as it helps bridge the digital divide [4]. Even with initiatives like the One Laptop per Child (OLPC), the penetration of the PC lags far behind that of the mobile phone [2]. According to the Tanzania Communications Regulatory Authority (TCRA); total subscriptions in Tanzania by March 2013 were around 27.6 million [5] as compared to 15 million subscribers in 2009 [6]. This shows that mobile technologies are rapidly being adopted (both locally and globally) and along with it; a significant growth in mobile services evolution.

The mobile phone is the device that people already carry at all times, and services beyond voice and text messaging are booming all over the globe [7]. The rate of development of the mobile phones in Tanzania opens a new service to the people; the most popular ones excluding the SMSs and voices services includes mobile money (M-Money) services offered by telecommunications operators and mobile banking (M-banking) systems offered by banking institutions. The first service includes Tigopesa, M-Pesa, Airtel money, EZY PESA provided by Tigo Tanzania Ltd, Vodacom Tanzania, Airtel Tanzania Ltd and Zantel respectively. The second service is offered by financial institutions that is the commercial banks, this includes: *Simbanking, and NMB Mobile* offered by *CRDB Bank Plc*, and *National Microfinance Bank* respectively [8]. These mobile services offer customer's convenience to access their financial resources timely and with much ease while the service providers generate some extra revenue. These services help in bridging the gap with rural area where there is no banking services [9]. The development of technology leads for the central bank of Tanzania to keep updating the payment systems in Tanzanian territory as explained in the next section.

2. PAYMENT SYSTEMS IMPLEMENTED IN TANZANIA

Central bank of Tanzania (BoT) is responsible for controlling all financial transaction in the country, this include defining the national payment system (NPS). BoT define NPS as a group of institutions and a set of instruments

and procedures, used to ensure the circulation of money within a country. The NPS supports the full spectrum of financial activity, from Tanzanian businesses transacting globally in the international markets to servicing the individual payment requirements of the Tanzanian populace [10]. Due to the technology development BoT keeps on updating various payment instruments into the system so as to ensure the national financial flow is stable. There are many national payment instruments being used in Tanzania, the most popular payment medium is cash. It is generally acceptable everywhere as a legal tender and is suitable for small value transactions. With the expansion of the economy and development of commercial banking, computer and communication technology, other non-cash payment instruments have been introduced. Non-cash instruments being accepted by the BoT to be used in Tanzania can be further classified as either paper based payment or electronic payment.

2.1 Paper-based payment instruments (PPI)

PPI include payment orders, bills of exchange, promissory notes and cheques. Automated credit transfers and direct debits are included in this mode of payment. Cheques remain the most frequently used non-cash payment instrument in Tanzania. According to [11], there are two types of cheques used in Tanzania for payment; Personal Cheques and Corporate Cheques, all type are physically rectangular in shape with different sizes and features. The major users of cheques are the Government departments, corporate bodies and individuals who deal with the government department and agencies [11]. Generally, few individuals write cheques mainly because personal cheques are normally not accepted due to among other reasons, the absence of unique personal identification. Only the Central Bank and commercial banks are allowed to issue cheques [11, 12]. Payments made by cheques had increased significantly since the automation of the Dar es Salaam Electronic Clearing House (DECH) on 1st February 2002 [12]. Paper based instruments for payment are used under the agreed terms and conditions between the customer and the bank. If there will be any violation on the agreed terms and condition will lead to one part losing her asset. However in most cases the customer becomes victim of the violation due to the fraud being committed to their bank account.

2.2 Electronic payment system (EPS)

Due to the development of communication systems, the BoT also had introduced different payment instruments based on the communication technology that is the EPS. BoT define EPS as any electronic instrument, device or system used for the purposes of facilitating payment transfers, through internet and/or wireless communication networks, and by use of service delivery products such as electronic cards, electronic payment transfers systems, mobile banking, Internet banking, automated teller machines, point of sales terminals, payment switches and any other type of electronic payment transfer system [10].

Electronic Funds Transfers (EFTs) - with the application of computers and communication technology, a number of paper-based payments have evolved into electronic forms, especially for large value transactions [12, 13]. EFTs is used for transferring value between banks on behalf of customers. Telegraphic Transfers (TTs) are the main forms of credit transfer [13, 14]. TTs are mainly used for wholesale payments. However, banks also utilize intra-bank communication networks using VSAT, leased lines and dial-up telecommunication systems to transfer inter branch payments electronically [13].

As Electronic commerce (EC) becomes a major component of business operations for many companies, EPS has become one of the most critical issues for successful business and financial services [15, 16, 17] EPS have several favorable characteristics including security, reliability, scalability, anonymity, acceptability, privacy, efficiency, and convenience [15, 16, 18]. EPS have gained recognition and have been deployed throughout the world [19].

Non cash payment is used mostly by organization to effects the large payments. The customer using this method had to adhere to the terms and conditions stipulated by the given bank. In electronic payment for example the Customer authorizes the Bank to act on and accept all instructions and transactions that occur after the customers PIN, Password or OTP have been entered or applied [20, 21]. The bank is entitled to and will proceed on under assumption that all such transactions have been authorized by the customer, even in circumstances where such transactions occur without the customers knowledge, consent or authority. Also If any unauthorized person obtains the Access Codes in any manner whatsoever, such a person will be regarded as the Customer's duly authorized agent with full authority to use the Electronic Channels Banking on the Customer's behalf, unless this is due to the Bank's negligence in which customer must prove beyond reasonable doubt [20, 21, 22, 23, 24].

Where paper based payment applied such as cheques also the terms and condition are clearly stated by the Tanzanian commercial banks. For example, in the use of cheques if all requirements are met the bank will make payment to the third party on behalf of the customer accordingly. The bank shall not be liable to the customer in any way and the customer shall fully indemnify the bank against any claims by any third party should the bank make payment against a cheque on the customer's behalf, where the cheque is presumed to be issued by the customer but the signature or content of the cheque and/or written instruction has been forged [20, 21, 24]. In case the customer wants the Bank to stop payment on a Cheque, the Customer must immediately request the Bank in writing to do so. Upon receipt of a written notice from the Customer to stop payment of a cheque, the bank shall record the notice and stop the payment provided that such notice is received before the transaction sought to be stopped has occurred [20, 21, 22, 23, 24].

This supported by The Bill of Exchange Act (Cap 215 R.E. 2002) section 60(1) thereof provides: "(1) when a bill payable to order on demand is drawn on a banker, and the banker on whom it is drawn pays the bill in good faith and in the ordinary cause of business, it is not incumbent on the banker to show that the endorsement of the payee or any subsequent endorsement was made by or under the authority of the person whose endorsement it purports to be, and the banker is deemed to have paid the bill in due course, although that endorsement has been forged or made without authority" It would appear from the provision of section 60 quoted above that banks are protected if in good faith and in the ordinary course of business it pays the instrument[25].

The customer is responsible for his/her bank account when there is any impersonification and forgery of the credentials that will make the bank to believe without doubt that the documents or information originates from their customer [20, 24]. These non-cash payment systems face a number of challenges related to customer bank account security ranging from risk behaviors done by users ignorantly, system availability, and some cases of fraud in which money vanish from customers' accounts without their knowledge. It is hard for the victim to identify when their accounts have been tapped or infiltrated. In order to avoid this trend and protect the customer from hackers there is a need of research to find the best secure approach for payment. This is the gap in knowledge which this study seeks to fill.

3. LITERATURE REVIEW

The victims of impersonification and forgery crime range from the individuals, Government departments/agents, private business organizations and Non-Governmental Organizations (NGOs) of mega fortunes. There have been a number of cases reported in Tanzania where customer's account were compromised by the fraudsters through stolen or forgery of credentials and managed to make some payment without the account holder consents [26].

In 2008, Barclays Bank Tanzania effected the transfer of 339 million Tanzania shillings from *Tourism Promotion Services (Tanzania) Limited* account to *East Africa Procurement Services Limited* account without a consent of the account holder. Barclays Bank Tanzania made the payment after receiving the document called *Request for Swift Customer Transfer Form* with all the requirements as per agreed terms and conditions. The bank had to effect the payment on behalf of her customer. However, the document was not originated from the real customer rather was forged [27].

In 2011, it was reported that the electronic transfer of money worth 400 million Tanzanian shillings from Vijana branch of CRDB bank in Dar Es Salaam to the customer account belonging to Marangu branch of the same bank in Kilimanjaro region. The fraudster managed to withdraw 35million Tanzania shillings from this illegal transaction before being detected and stopped by the bank [28]. This indicates that once someone gains the customer credential can manage to make payment without the owner of the account knowledge [29].

Also, a similar case in 2010 where by more than half a billion Tanzanian shillings were transferred from CRDB bank to NBC and converted into mobile phone vouchers immediately [30]. This was reported in 2011 where electronic means of payment was used. However; the point here is not how the money was spent rather how it swiftly changed accounts without the consent of account holders. With these cases the customers are at risk of losing their asset where the agreed terms and conditions apply. For example, when the electronic channel is used to effect the payment, the customer authorizes the Bank to act on and accept all instructions and transactions that occur after the customers PIN, Password or OTP have been entered or applied [20, 21, 22, 23, 24]. The bank is entitled to and will proceed on the assumption that all such transactions have been authorized by the customer, even in circumstances where such transactions occur without the customers knowledge, consent or authority. [20, 21, 22, 23, 24, 30]

However most of the cases are underreported by the financial institution in Tanzania due to the fear of losing reputation before customers [31]. Most of the officials in those institutions who did not want their name to be mentioned to secure their jobs admitted that a lot of such frauds in customer's account still happening. It was also reported that cases of fraud and Cyber-crime costs East African countries billions of dollars but the rackets remain shrouded in secrecy because the affected companies prefer to suffer in silence, 'safeguarding' their reputations [26, 31]. The underreported cases make difficult in assessing the level of the transaction security [31, 32]. This problem is growing every day in Tanzanian banks as technology advances and people decide to misuse it for earning income illegally. People have experienced fraudulent behaviors over the Internet including fraudulent emails, credit card fraud and unauthorized bank transfers [31, 33].

As customer needs to adhere to the banks terms and conditions thereby it is proposed a method that can address this problem by adding security features via mobile phone. This paper proposes the method to be employed by the financial institutions in Tanzania to increase the security by improving authentication of the customer's while accessing their accounts. All non-cash payments should be included in this proposed method as it is subjected more to frauds threats.

4. SECURITY FEATURES IN NON-CASH PAYMENT INSTRUMENTS

There are many non-cash payments instrument being accepted by the BoT as explained earlier. In each of these instruments, there are security features that help in reducing the fraudulent of the customers' assets. The security features vary from one instrument to another.

The Cheque

Banks and their corporate customers who print their own cheques, the following security features are applied to their printed cheques in order to detect any fraudulent alterations and counterfeiting:

a. *Paper type:* the cheque paper used must be CBS1 paper, which are dull under ultra violet light, i.e. it does not fluoresce or brighten when tested under ultra violet light.
b. *Watermark:* All cheques carries a standardized watermark applied at paper manufacturing stage, with the word "TACH" surrounded by a circle with diameter of 4.5 cm, which is seen when held against any light source. Each cheque has at least one full watermark as seen in the figure 1 below.

Figure 1. A standard Cheque watermark [11]

c. *Micro-texting /Micro-lettering:* the banks must use micro-text in areas that are susceptible to alterations. The line to fill in the payee's name and the amount in words must have the bank's name written in micro letters, which are visible to the naked eye only under a magnifying glass.
d. *Bank's logo printed with ultra-violet ink:* The bank's logo printed in ultra-violet (UV) ink must be included. The logo is captured by/visible in UV enabled scanners/lamps.
e. *Bleeding ink:* The use of bleeding-Ink on MICR code line ensures that the code line is visible through the paper, both at the front and the back of the cheque [11].

The above features are mandatory in accordance with BoT cheque standardization in Tanzania. Not only that but also the draft of cheque must have features as shown in a corporate cheque draft below Figure 2. Any cheque draft must include the listed features including the signatures specimen of the corporate signatories.

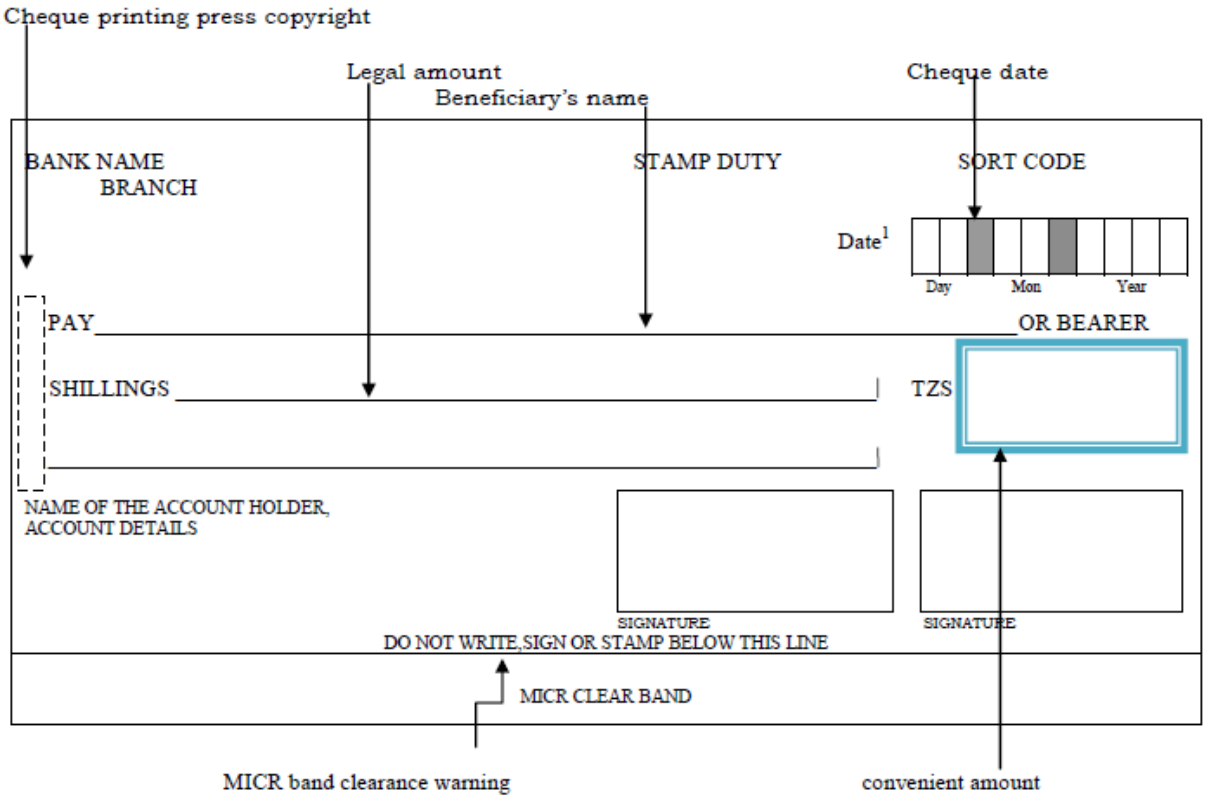

Figure 2: General Cheque layout – Corporate cheque [11]

For security purposes when writing a cheque, always a customer has to take care by filling in the details in a way that will be difficult for other person to alter. For example do not leave gaps between the words and figures, begin the amount in words as close as possible to the left hand side and fill in the amount in figures as close as possible to the TZS

sign. Never fill out a cheque in pencil or ink that can be erased and never sign a cheque before it is completely filled out [34].

Generally the entire paper based payment instrument being agreed between the customer and the bank must have the signature specimen as agreed by both actors. For the payment to be made the instrument must have fulfilled all the requirements as per term and conditions being stipulated thereof.

Electronic Payment System

In this kind of payment generally the security features includes the user ID, Password, secret words, fingerprint etc depending on the application the given bank uses to secure their customers assets. When the information on transaction fulfills the requirements the bank perform the transaction on behalf of the customer according to the instruction being given by their customer. This is done under assumption that the instruction has been originated from the customer even if it's not [13].

5. THE CURRENT OPERATIONS TO EFFECTS PAYMENTS BY NON-CASH PAYMENT INSTRUMENTS

Generally the procedures to effect payment using non-cash payment instruments are similar in all tools though sometimes there some little differences in the process. However the main areas to be checked are the same. For example in all tool used to effect payment usually must meet the requirements such as the security features like password, signatures, account numbers, account holder names, etc. In this paper we demonstrate the use of Cheque instrument to represent the rest of tools as it is the most used in non-cash payment instrument in Tanzania.

Processing Cheques for Payment

Most people (organization) who receive cheques (payees) deposit them with their own financial institution. Usually after filling the deposit cheque form their account will be credited immediately and an electronic payment record containing details from the cheque is created and sent to the cheque writer's (payer's) financial institution. The payer's account is then debited if the cheque is to be paid by the payer's financial institution. The figure 3 below shows how the cheque is processed if the payee and payer are not using the same financial institution (Bank) [34].

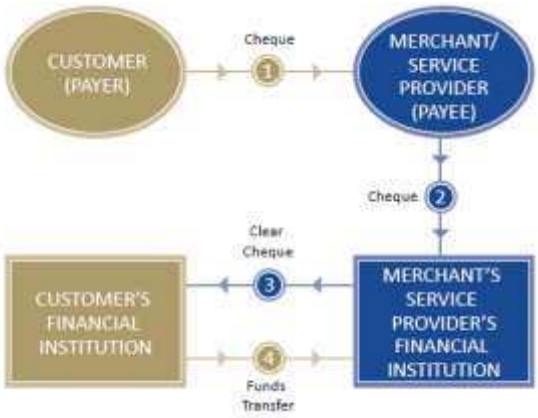

Figure 3: Cheque processing when payers and payee use different banks [27]

When you issue a cheque, you are giving your financial institution written instructions to pay a specific amount from your account. The cheque clearance cycle makes it possible for financial institutions to complete the necessary checks to make sure payment is made in accordance with your instructions. Since cheques are a paper based payment instrument, they need to be physically presented to the financial institution they are drawn on for payment decisions. As part of the clearance cycle, the cheque you deposit is physically transported from your financial institution to the financial institution where the payer's account is held and the payer's instructions are verified. The payment record that is electronically transmitted to the payer's financial institution speeds up the process of checking that there are sufficient funds available in the account to make payment. In this case if there is insufficient fund the cheque will be dishonored. However, the cheque can be still dishonored for other reasons for example, if it is not signed in accordance with the authority held at the financial institution. Figure 4 below shows how the current information flows when the non-cash payment instrument is used to effect the transaction [35]

International Journal of Information and Communication Technology Research

http://www.esjournals.org

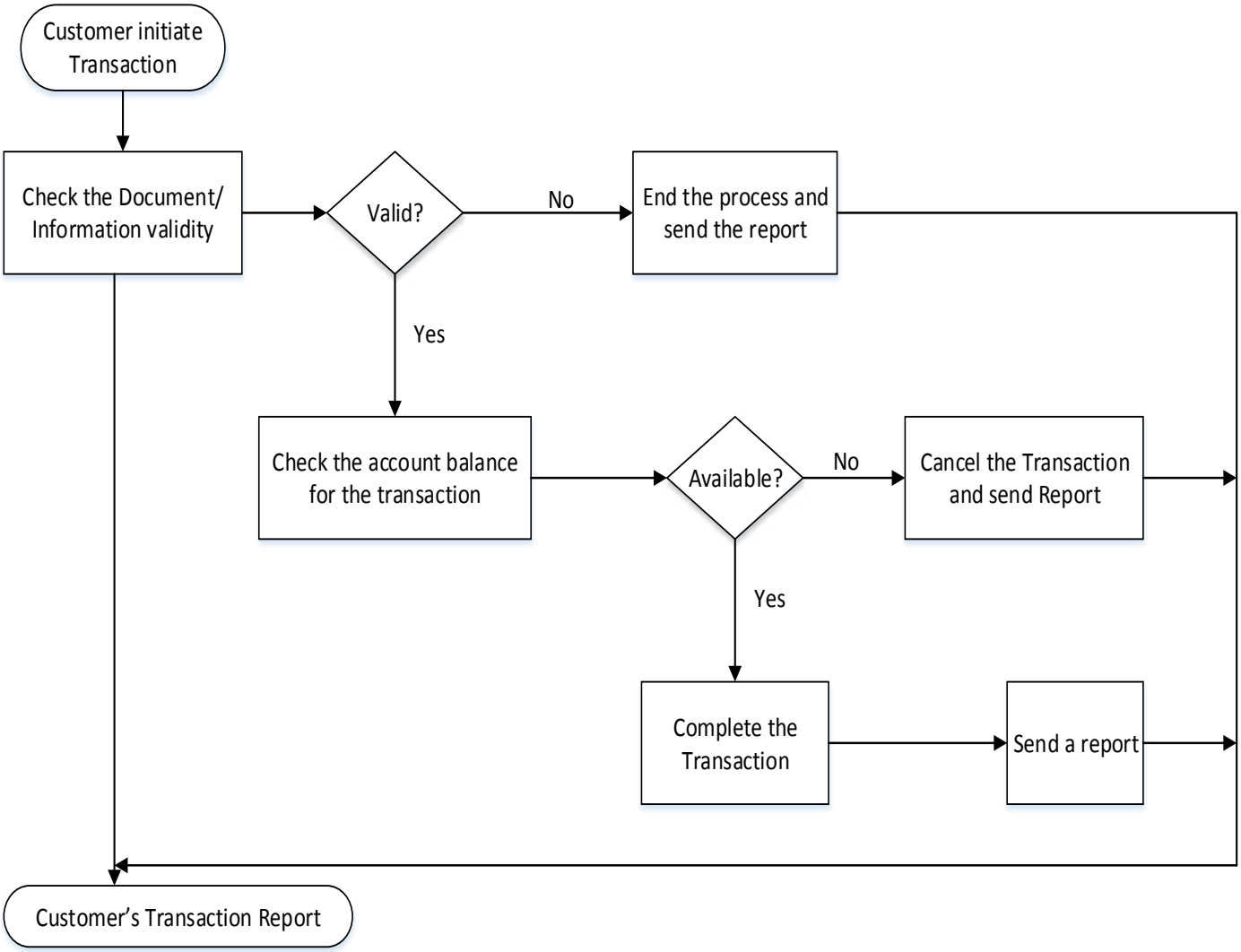

Figure 4: Information flow for Non-cash payment instrument in Tanzania [28]

As it is demonstrated above the customer initiate the payment transaction by any means, in this case the cheque is being used. The instrument will be physically presented to the bank where the security and other features have to be checked for its validity. When this step is cleared the bank have to make sure that the payers' account has enough balance to effect the transaction. If there is enough balance to effect the transaction then the bank will make payment according to the payer's instructions. The report will be generated to be reflected in the monthly bank statement of the payer's bank account. It should be noted that the banks set their own procedure on how to clear the cheque before being paid [35].

However passing all the steps doesn't meant that everything will be okay sometimes the cheque can be dishonored [34]. A cheque may be stopped for many reasons, but most often, because it has been reported as lost or stolen by the payer. If you are given a cheque and subsequently lose it or believe it has been stolen, you should contact the payer immediately. The payer will then instruct his or her financial institution to put a stop payment on the cheque. Similarly, if you issue a cheque and then decide to stop payment, you should contact your financial institution immediately and provide full details of the cheque. In case the cheque has not already been

paid, the paying financial institution will dishonor it when it is presented for payment [20, 21, 22, 23, 24].

6. PROPOSED MODEL TO ADDRESS THE PROBLEM OF IMPERSONATION

The main purpose of the proposed security model in banking systems in Tanzania is to protect the banks customer from any form of threats that endangers their assets. These threats include [36]:

a. Identity theft and Documents forgery

Identity theft refers to all types of crime in which someone illicitly obtains and uses another person's personal data through deception or fraud, typically for monetary gain. Identity theft occurs through a wide range of methods from very low-tech means, such as cheque forgery and mail theft to more high-tech schemes, such as computer spyware and social network data mining [37, 1]. It's common in Tanzania for someone to make a forgery in documents so as to gain an illegal access to the account information of the customer [36, 38]. Commonly payment instruments subjected to this threat among others includes bank cheque, payment orders, bills of exchange, and promissory notes. As it stipulated in literature reviews many reported case were due to this kind of threat which leads to the loss of the customers assets.

b. Password Database Theft

Stolen user credentials are a valuable commodity and, often times, cybercrime rings operate solely to obtain this information and sell it to the highest bidder or use it themselves to access user accounts [36, 38]. This puts the online banking customer into risk as someone can have an access to his or her account without their consent. Hackers steal user data and passwords from one Web site operator to hack other sites. Since many people use the same user ID and password combination for multiple sites, the attacker can hack additional accounts that the user has.

c. Man-in-the-Middle (MitM) attack

In this type of threat, the attacker can actively inject messages of its own into the traffic between the user's machine and the authenticating server. One approach for MitM attacks involves pharming, which involves the usage on malicious network infrastructures, such as malicious wireless access points or compromised DNS servers, to redirect users from the legitimate site they are trying to access to a malicious fraudulent Web site that accesses the user credentials and acts on behalf of the user to perform malicious activities [36].

d. Phishing

Although passwords can also be obtained through less sophisticated means such as eavesdropping, guessing, dumpster diving, and shoulder-surfing, phishing is a common form of cybercrime typically carried out through e-mail or instant messaging, providing links or instructions that direct the recipient to a fraudulent Web site masquerading as a legitimate one [36 37]. The unsuspecting user enters personal information (such as user names, passwords, Social Security Numbers, and credit card/account numbers), which is then collected by the hacker. Of particular attraction to phishing scams are online banking, payment services, and social networking sites. According to the Gartner survey [39] phishing attacks continue to exact financial damage on consumers and financial institutions, with a trend toward higher-volume and lower-value attacks. The survey found that more than five million U.S. consumers lost money to phishing attacks in the 12 months between September 2007 and 2008, a 39.8% increase over the number of victims a year earlier.

6.1 General structure of the proposed system

The prevailing of the fore mention threats on customer accounts needs a system that can solve it. The availability of mobile phones technology which is dominating the communication market; the technology can be used for many purposes beyond the voice services and Short Message Service *(*SMS). Therefore the mobile phone can be utilized to secure the user bank account as being proposed in this paper. It can help to either eliminate or reduce the problem by designing the system that requires account holders to provide final authentication of any transaction involving withdrawal of the money from their account through the use of their mobile phones being registered at the given bank.

Therefore, the structure of the proposed system is based on the three tiers involving the client, application server and the banking core database server. In this system, the client/customer is linked with the mobile communication system for the final authentication. The proposed system mainly focuses on the authentication of the customer using multiple authentication factors implemented in tools which are faster and cost effective. The general architecture for the proposed system is shown in the Figure 5.

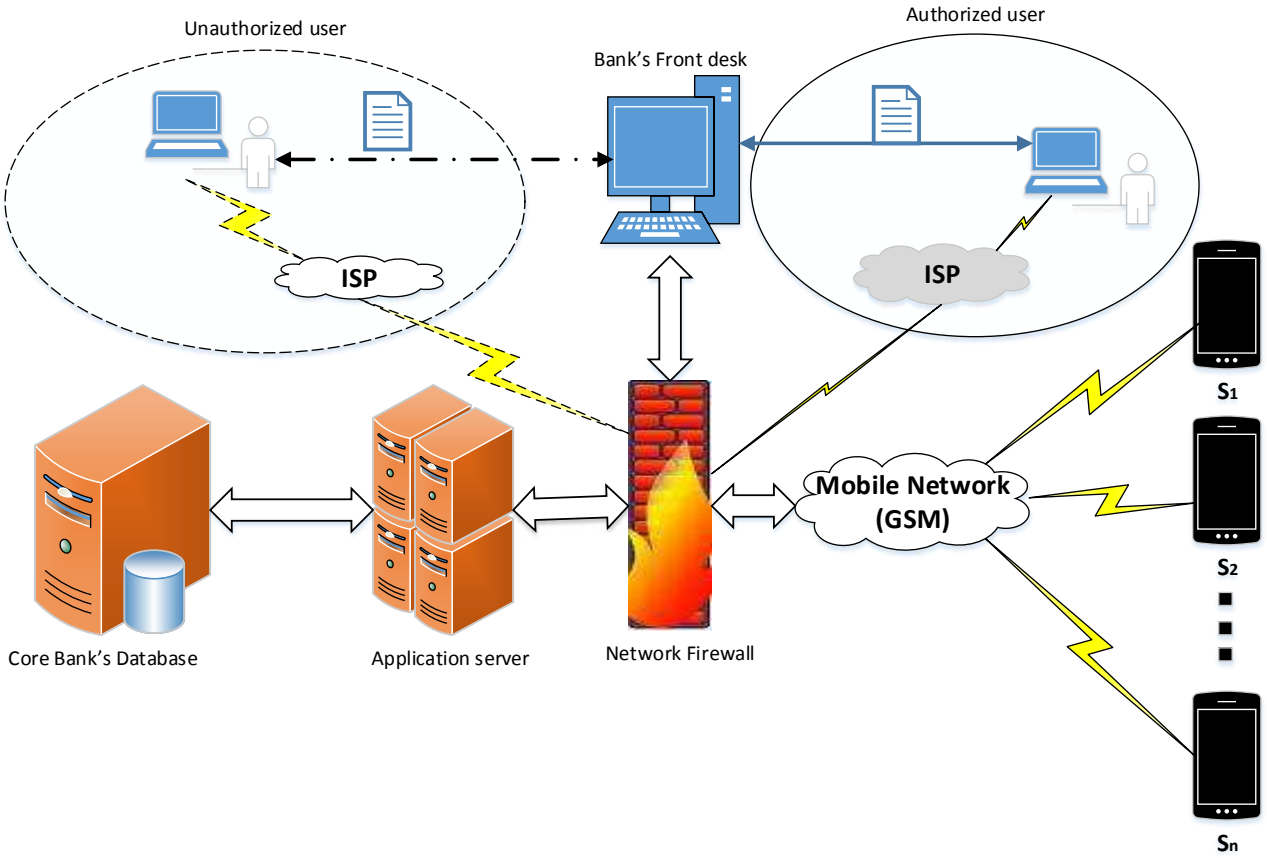

Figure 5: General architecture of the proposed system

The client/Customer

The client/customer is the initiator of any transaction in the bank account being owned by them. The client includes all authorized user in the concerned bank account. In this process a client must ensure that all the agreed requirements with his bank are fulfilled depending on the payment instrument being used. If paper based tools are used the client initiate the transaction through bank's front desk which provokes the application server on the customers behalf. If electronic instrument being used the client himself initiate the transaction in the application server passing through the banks firewall.

Application Server

The application server receives the incoming requests from the banks network and upon receiving one; it decodes it into some interpretable format. It then uses the designed protocol to perform the initial security checks on the received request before generating the security message to be sent to the customer via mobile network for the final approval. The application server generates a secured message and sends it via GSM network to the customer mobile phone that captures the security details of the transaction to be done and generate the secured message to be sent back as response from the client. This component can be located and administered by a particular application vendor or it can be independently located and administered by the bank itself. It initiates the communication with a banking system that contains a database that has all the banking and security details of the users.

The core Bank database

In the core database Customer's banking details, security details, and other related user information are kept. The information's are being utilized by the Application server for customer verification and execution of the various requested transactions.

The security of the communication between the bank system and the client via GSM networks will be taken care by the *Enhanced Security Model* being proposed by [8] in the paper titled *Enhanced Security Model For Mobile Banking Systems In Tanzania.* In their proposed model, the GSM networks act as carrier of the message and they should not know the content of the message. It was also shown that even a third part managing to capture the transmitted message through the GSM Networks won't be able to view the

content it carries. Their model overcomes the security weaknesses of the GSM Networks.

6.2 General Information flow in our Proposed System

The proposed system is based on the non-cash payment instruments being used by the customer to effect payments from their banks accounts. Generally the customers present the payment instrument (paper based e.g. Cheque) to the Bank's front desk where the documents are verified for its validity. After the validation the bankers will initiate the system for payment in the application server via the banks firewall up to the core banking server. In case of the electronic instruments being used, the customer will initiate the transaction through internet where the information had to be send to the application server via Bank's firewall where the security credentials will be verified before the transaction is allowed to proceed to the next stage. For security purposes all information will be passed through the banking firewall before communicated to the applications and the core banking server. The information flow for the proposed method is as shown in the flow chart below. All the current procedures are maintained and an additional feature is added to strength the authenticity security to the banks account of the customer.

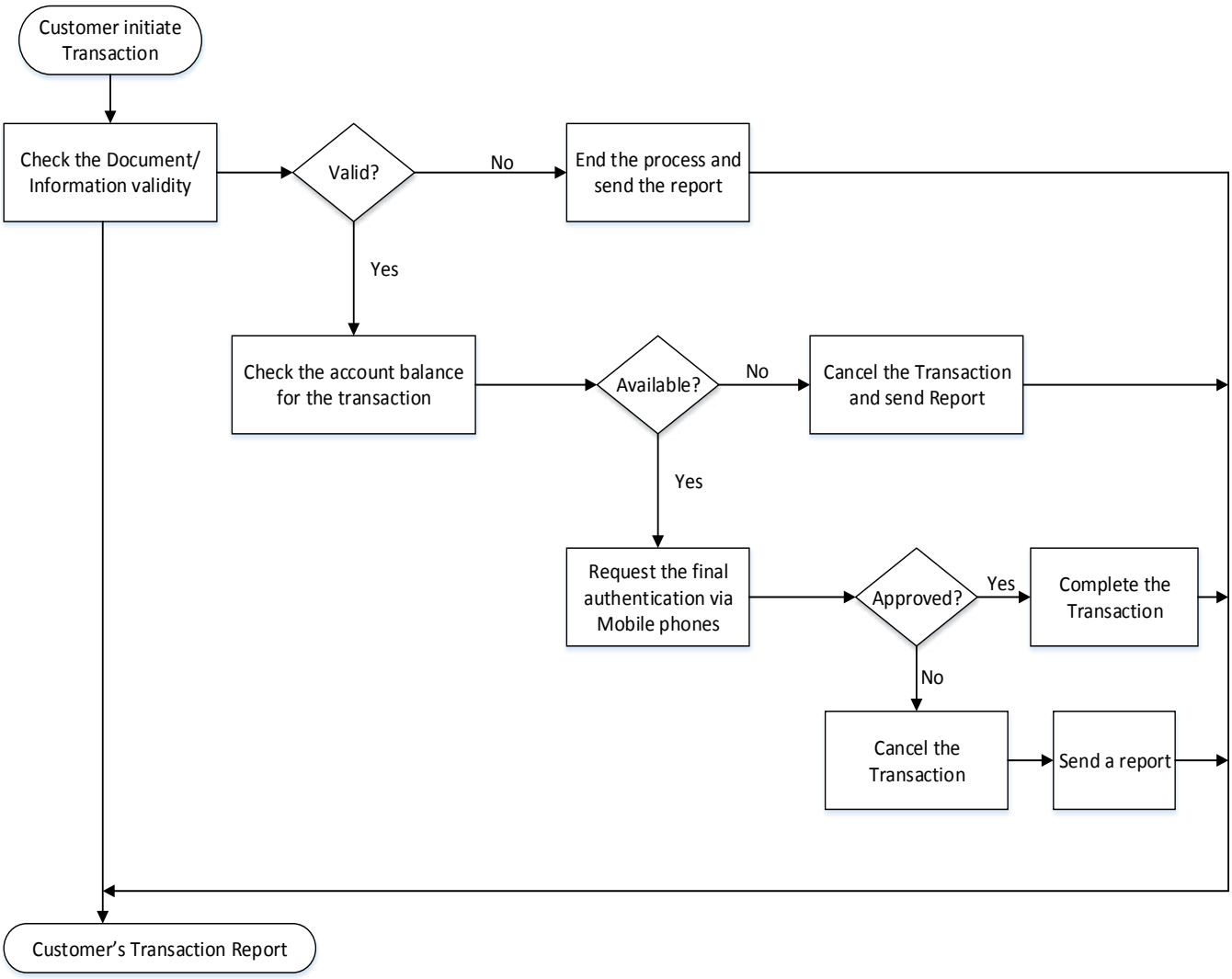

Figure 6: General Information Flow for the proposed system

As indicated in Figure 5 after the initial security checks and ensuring that the fund for the said transaction are available the application server will generate a secured message and send it via GSM network to the mobile phones of the registered signatories' (S_1, S_2, … S_n) of the payer. The purpose of this message is to request the final authentication

of the transaction to be done. The payment will be effected only when the signatories provide a final approval of the transaction via their register mobile phones otherwise the transaction will be cancelled. In this system, it doesn't matter who initiated the payment transaction and which payment instrument being used; the final authentication through mobile phones is a mandatory to effect the payment.

6.3 Authentication process in a proposed model

The methods in which somebody could be authenticated fall into three categories, based on what are known as the factors of authentication. These factors include something the user *knows* (e.g., password, or personal identification number (PIN) etc.), something the user *has* (e.g., ID card, security token, cell phone etc.), and something the user is (e.g., fingerprint, retinal pattern, DNA sequence etc.) [40, 41].

The authentications process can include one of the above mentioned factors if only one component is used as a means of verifying customer identity; it is termed as Single-factor authentication. It is an easy way for customer to remember though if the component has been compromised the possibility of the user to lose the asset is very high [42]. Two-factor authentication potentially provides enhanced security by combining two different authentication components; the advantage being that security can be maintained by one of the components if the other component is compromised [41, 43].

For a positive and strong authentication, the security research has determined that elements from at least two, and preferably all three, factors should be verified however in General, the multifactor authentication that combines all three factors has not been widely applied [40, 41, 42]. To adhere with these research findings, the proposed system embeds all the three factors for authentication.

In proposed system the customer mobile phone number being registered at the bank which fall under the something the user has, during the process of authentication the generated message will be send to the registered number with the detail of the requesting transaction. Upon the agreement or accepting the transaction as being originated from them then the customer will be required to enter the password, which is something the user knows. When the password is verified to be genuine the system will need to verify if the person responding to the real time messaging is the one known with the bank. This process will be done by capturing the finger print through the use of the mobile phone touch screen/camera, this determine something the user is. The authentication process of the proposed system has been depicted in the Figure 7.

6.4 The assumption made under the proposed system

The assumptions that were made in designing the proposed solution are as mentioned below:

- **a.** All signatories work in good faith to serve the interests of their company/institution and no personal interest being entertained.
- **b.** It assumed that the bank distribute the application to its customers handsets to ensure the security compatibility in their systems.
- **c.** It is also assumed that the message from the bank institution will be given higher priority by the mobile operators so as to ensure the messages are delivered on time at high speed (real time).

7. CONCLUSION

The mobile based authentication system has being presented in this paper which focus on the securing the customer banks account. The model requires all the transaction from the customer by any payment instrument used; it must get the final authentication from the registered mobile phones. If the system is implemented some threats will be minimized if not eliminated or reduced, these threats includes: phishing, identity theft, document forgery and man at the middle. The system includes all the available security features and implements the authentication feature through the use of the mobile phones of the customers' signatories. The focus of the future research will be to work on the implementation of the proposed system in the real environments to enhance the added security features of the system.

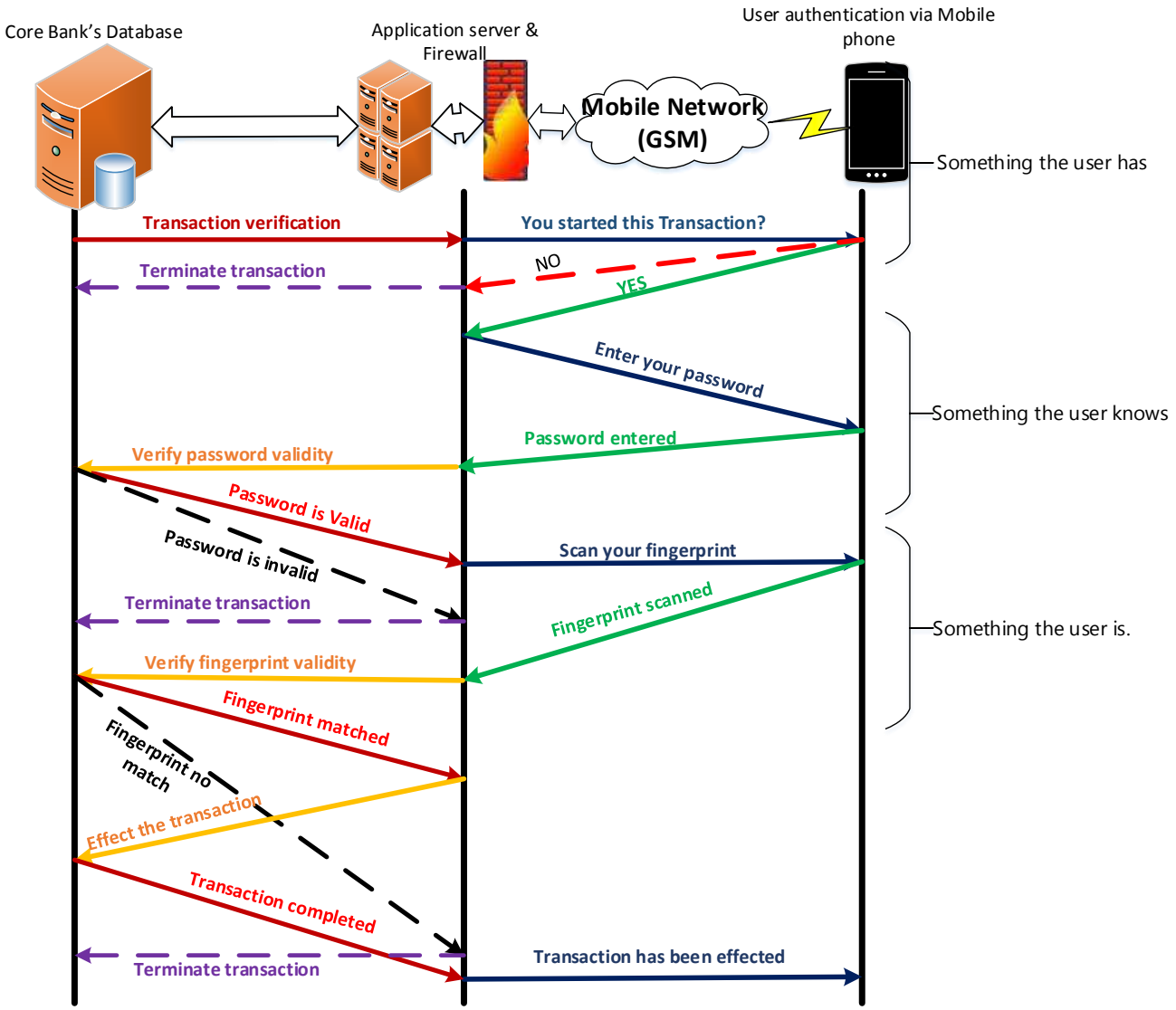

Figure 7: The authentication process of the proposed system

REFERENCES

[1]. Kim W, Ok-Ran J, Chulyun K, Jungmin S, The dark side of the Internet: Attacks, costs and responses, Journal of *Information Systems, Volume 36, Issue 3, May 2011, Pages 675-705*

[2]. Gelmato, (undated) Mobile Banking Product Overview, Security to be free, Available at: http://www.gemalto.com/brochures/download/mob_banking_product.pdf Accessed on 24th August, 2014.

[3]. Howcroft, B., & Durkin, M. (2000). Reflections on bank-customer interactions in the new millennium. Journal of Financial Services Marketing, 5(1), 9–20.

[4]. Streicher-Porte M, Marthaler C, Böni H, Schluep M, Camacho Ál, Hilty L. M, One laptop per child, local refurbishment or overseas donations? Sustainability assessment of computer supply scenarios for schools in Colombia, *Journal of Environmental Management, Volume 90, Issue 11, August 2009, Pages 3498-3511*

[5]. TCRA. Telecommunications Statistics March 2013. 2013; Available at: http://www.tcra.go.tz/images/documents/telecom

munication/telecomStatsMarch13.pdf Accessed on 15th August, 2014.

[6]. IST-Africa. Introduction - Republic of Tanzania. 2010; Available at: http://www.ist-africa.org/home/default.asp?page=doc-by-id&docid=4324; Accessed on 14th August, 2014.

[7]. Gelmato, (undated) Mobile Banking from a world leader in digital security: - Providing secure and easy access to banking services anytime, anywhere, Available at: http://www.gemalto.com/brochures/download/mobile_banking.pdf Accessed on 24th August, 2014.

[8]. Nyamtiga, B. W, Sam A, Laizer L. S, Enhanced Security Model For Mobile Banking Systems in Tanzania, International Journal of Technology Enhancements and Emerging Engineering Research, VOL 1, ISSUE 4 (2013), ISSN 2347-4289. Available at: http://issuu.com/ijteee/docs/enhanced-security-model-for-mobile-/1; Accessed on 22nd June, 2014.

[9]. David A. Helton, Bridging the digital divide in developing nations through mobile phone transaction systems, Available at: http://www.westga.edu/~bquest/2012/divide2012.pdf Accessed on 23rd August, 2014.

[10]. BoT, NPS - Frequetly Asked Questions, http://bot.go.tz/PaymentSystem/FAQ.asp Accessed on 10th august 2014.

[11]. BoT TACH, (2013) Cheque Standards and Specifications, available at: http://bot.go.tz/PaymentSystem/Cheque%20Standards%20and%20Specifications%202013.pdf Accessed on 14th January, 2014.

[12]. BoT, (2003) Payment Systems in The Southern African Development Community - Tanzania Chapter, available at: https://www.bot-tz.org/PaymentSystem/Green%20book%20draft%2003dec-final.pdf Accessed on 4th May, 2014.

[13]. BoT, (2007), Electronic Payment Schemes Guidelines, available at: http://www.bot-tz.org/paymentsystem/Docs/e_Schemes%20Guidelines%20June%202007.pdf Accessed on 24th July, 2014.

[14]. NPS Newsletter April, 2007, Available at: http://www.bot-tz.org/paymentsystem/NewsLetters/MALIPO%203rd%20%20Issue.pdf Accessed on 12th April, 2014.

[15]. Kousaridas, A., Parissis, G., and Apostolopoulos, T., An open financial services architecture based on the use of intelligent mobile devices, *Electronic Commerce Research and Applications, 7, 2008, 232–246*

[16]. Cotteleer, M. J., Cotteleer, C. A., and Prochnow, A. Cutting checks: challenges and choices in B2B e-payments. *Communications of the ACM, 50, 6, June 2007, 56–61.*

[17]. Peha, J. M., Khamitov, I. M. PayCash: a secure efficient internet payment system, *Electronic Commerce Research and Applications, 3, 2004, 381–388.*

[18]. Tsiakis, T., Sthephanides, G. The concept of security and trust in electronic payments, *Computers and Security, 24, 2005, 10–15.*

[19]. Changsu K., Tao W., Namchul S, Ki-Soo K. An empirical study of customers' perceptions of security and trust in e-payment systems, *Electronic Commerce Research and Applications, Volume 9, Issue 1, January–February 2010, Pages 84-95*

[20]. Barclays BankTanzania Limited, Terms and conditions between the Customer and the Bank , Available at: http://www.barclays.co.tz/corporate/internet-banking/terms-conditions/index.html , Accessed on 19th August, 2014.

[21]. NBC, Terms & Conditions for Electronic Banking Channels 2013, available at:http://www.nbctz.com/downloads/terms/eng.pdf Accessed on 19th August, 2014.

[22]. NMB, Terms and conditions between the Customer and the Bank, available at: http://www.nmbtz.com/index.php?option=com_content&view=article&id=272 Accessed on 19th August, 2014.

[23]. CRDB Bank PLC, General Terms and Conditions for Operating With CRDB Bank PLC, Available at: http://www.crdbbank.com/index.php?option=com_phocadownload&view=category&download=53:general-terms-and-conditions&id=2:account-forms&Itemid=158 Accessed on 19th August, 2014.

[24]. I&M bank Tanzania, General Terms & Conditions for our various services, Available at: http://www.imbank.com/tz/terms-and-conditions-2/terms-and-conditions/ Accessed on 19th August, 2014.

[25]. The Bill of Exchange Act (Cap 215 R.E. 2002), available at: http://www.comcourt.go.tz/comcourt/download/act/The%20Bills%20of%20Exchange%20Act,%20Cap.215%20R.E%202002.pdf Accessed on 25th June, 2014.

[26]. Daily news (6th May 2011), "E. A. countries lose billions from fraud, cyber-crime", Daily News Media Group, available Tanganyika National library Dar es Salaam.

[27]. The citizen (Tuesday, 27 July 2010) Sophia Mtiiye and Bernard James, "Six in court on Sh339m fraud charge", Mwananchi Communications Limited, available Tanganyika National library Dar es Salaam.

[28]. Mwananchi **(**Monday, 03 January 2011**)** "Mafia Fraud waves the CRDB Bank", Mwananchi Communications Limited, available Tanganyika National library Dar es Salaam.

[29]. Center for Identity Management and Information Protection Utica College, types of identity crimes, available at: http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm Accessed on 25th August, 2014.

[30]. This day (2nd February 2011) "Police uncover massive money-laundering scam" Media Solutions Ltd: http://www.thisday.co.tz/?l=11017 Accessed on 18th August, 2014.

[31]. Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania?. *International Journal of Information Security Science*, *3*(2), 182-199.

[32]. M. A. Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, *Journal of International Commercial Law and Technology* Vol. 5, Issue 4 (2010)

[33]. The citizen (Monday, 11 July 2011) "CRDB**:** We've increased client protection against cybercrime**",** Mwananchi Communications Limited, reported By Victor Karega, available Tanganyika National library Dar es Salaam.

[34]. APCA, Cheque Fact sheet, Available at: http://www.apca.com.au/docs/about-payments/cheque_fact_sheet.pdf Accessed on 5th August, 2014.

[35]. White paper Top Online Banking Threats to Financial Service Providers in 2010 http://www2.safenet-inc.com/email/2010/MITB-2010/WhitePaper_Top-Threat-to-Financial-Service-Providers-in-2010_FINAL.pdf; Accessed on 13th February, 2014.

[36]. FATF Report (2010) Money Laundering Using New Payment Methods, Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ml%20using%20new%20payment%20methods.pdf Accessed on 25th August, 2014.

[37]. Khonji M, Iraqi Y, Jones A, Phishing Detection: A Literature Survey, IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013, pages 2091- 2121.

[38]. Gartner, Inc. "Banks Need to Strengthen User Authentication While Appeasing Consumers." May 2008. ID G00158229

[39]. Wikipedia, Authentication, Available at: http://en.wikipedia.org/wiki/Authentication#cite_note-2 Accessed on 25th August, 2014.

[40]. Federal Financial Institutions Examination Council (2008). "Authentication in an Internet Banking Environment". Retrieved 2014-08-25 at: http://www.ffiec.gov/pdf/authentication_guidance.pdf Accessed on 25th August, 2014.

[41]. Gunson N, Marshal D, Morton H, Jack M, User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking, Computers & Security, Volume 30, Issue 4, June 2011, Pages 208-220

[42]. Toledano DT, Fernandez P. R, Hernandez T.A, Hernandez G. L, Usability evaluation of multi-modal biometric verification systems. Interacting with Computers September 2006; 18(5):1101-22.

[43]. O'Gorman L. Comparing passwords, tokens and biometrics for authentication. Proceedings of the IEEE December 2003; 91(12):2021- 40.