Tanzania Journal of Science 46(3): 791-806, 2020
ISSN 0856-1761, e-ISSN 2507-7961
© College of Natural and Applied Sciences, University of Dar es Salaam, 2020

Security Model for Tracking Creation of Mobile Money Using Transport Layer Security Protocol

Sigsbert Rwiza[1*], Mussa Kissaka[1] and Kosmas Kapis[2]
[1]Department of Electronics and Telecommunications Engineering, College of Information and Communication Technologies, University of Dar es Salaam, P. O. Box 35062, Dar es Salaam, Tanzania
[2]Department of Computer Science and Engineering, College of Information and Communication Technologies, University of Dar es Salaam, P. O. Box 33335, Dar es Salaam, Tanzania
**Corresponding author e-mail address: rwiza2010@yahoo.com*
Co-authors e-mail addresses: mkissaka@yahoo.com, kkapis@gmail.com

Received 20 July 2020, Revised 16 Sept 2020, Accepted 6 Oct 2020, Published Oct 2020
https://dx.doi.org/10.4314/tjs.v46i3.19

Abstract

Mobile Network Operator (MNO) financial service model has security vulnerabilities in addressing verification of cash and mobile money. For instance, monthly returns are transferred in plain text from banks and MNOs to financial regulators. This may result to failure of financial regulators in detecting creation of fake mobile money. This study was conducted to develop a security model for tracking creation of mobile money using Transport Layer security protocol as a way of protecting returns in transit from banks and MNOs to financial regulators. The proposed model was developed using insights from literature, function decomposition and composition techniques and was tested by prototyping the system for tracking creation of mobile money using Laravel PhP framework, apache webserver, JavaScript Object Notation (JSON) server and PhP programming language. The proposed model has eight components, namely; certificate authority, financial regulator server, bank server, MNO server, bank system, mobile money system, super-agent and mobile money issuer components.

Keywords: Security Model, Public Key Infrastructure (PKI), Tracking Creation, Transport Layer Security, Mobile Money.

Introduction

Mobile money services in the world have expanded rapidly due to Mobile Network Operator (MNO) financial service model (Castri and Gidvani 2014). Mobile money being electronic money generated by the mobile money system may be genuine or fake (Rwiza et al. 2020). The genuine mobile money is generated when super-agent deposits money in MNO trust account while fake mobile money is generated without depositing equivalent money in the trust account. Financial regulators have put in place electronic money regulations for managing risks related with creation and issuance of mobile money (Rwiza et al. 2020). One of the risks in the creation and issuance of mobile money is the creation of fake mobile money.

Financial regulators track creation of mobile money for managing related risks. For the past decade, creations of mobile money have boosted financial inclusion in rural and urban areas. Financial regulators track creation of mobile money based on returns from banks and MNOs. The returns from banks are amounts of deposited money into trust account, the name of super-agent, the issuer of mobile money (MNO) and the transaction reference number. The returns from MNOs are amount of issued mobile money, name of super-agent issued with mobile money, name of mobile money issuer (MNO) and transaction reference number.

The study conducted by Rwiza et al. (2020) in Tanzania, Uganda and Kenya revealed that returns from banks and MNOs to financial regulators are carried in plain texts. Returns are prone to modification by adversaries and may be exposed to unauthorized entities along the way from banks and MNOs to financial regulators. In MNO financial service model, the major security risk is the regulator receiving fake returns (data) from banks and MNOs or receiving returns from wrong senders or receiving incomplete returns (Nyamtiga et al. 2013). Such security threats can lead the failure in detecting creation of fake mobile money.

A security model for tracking creation of mobile money is required for assisting financial regulators to manage integrity, confidentiality, non-repudiation and authentication security risks as returns are transferred from banks and MNOs to financial regulators. One way of establishing security models is by using the Public Key Infrastructure (PKI) (Misra et al. 2015). PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communication and business transactions on networks (Al-Janabi and Obaid 2012). It is implemented using various security protocols including Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. SSL versions and TLS versions lower than TLS 1.3 have been found to have security vulnerabilities such as man-in-the middle and drop change cipher spec attacks (Curguz 2016).

Researchers have revealed that TLS 1.3 protocol is the appropriate protocol for securing communication over the internet (Houmani and Debbabi 2012). To implement TLS 1.3 using PKI, a Certificate Authority (CA) has to be installed and configured (Latif et al. 2018). TLS 1.3 protocol has handshake and record protocol. The handshake protocol helps in session establishment in which systems validate each other before sharing data. The record protocol is concerned with data transfer when systems have validated each other. As indicated in Figure 1, in record protocol, the Hash-based Message Authentication Code (HMAC) function is used to achieve integrity, confidentiality and non-repudiation security services (Latif et al. 2018).

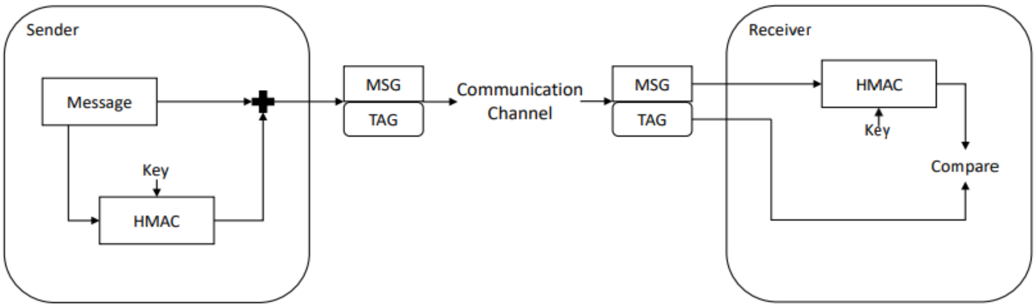


Figure 1: Enforcing data integrity and confidentiality using HMAC function (Latif et al. 2018).

The architecture in Figure 1 was adapted in the use of HMAC function to enforce integrity, confidentiality and non-repudiation security services. In the context of this study, the sender passes the data through HMAC function to obtain the digest. The sender signs the digest using own private key. The sender encrypts the original data using the public key of receiver. The signed digest (TAG) and cipher text (MSG) are sent to the receiver. At the receiver, the signed digest is verified using the public key of the sender. The cipher text is decrypted using the private key of receiver; the obtained plain text is hashed using the HMAC function. The two hashes are compared; in case they are equal then this is the proof that the data received by the receiver were totally sent by the sender and were not modified while in transit.

This study was conducted to develop a security model for tracking creation of mobile money using TLS 1.3 protocol. The BiBa and the Bell-Lapadula models offer integrity and confidentiality measures as an alternative to improve the security of information in organizations. However, they are not designed for tracking creations of mobile money in information systems (Toapanta et al. 2018). The study conducted by Zhao and Chadwick (2008) on modeling of Bell-LaPadula security policies using Role Based Access Control (RBAC) has implication to this study. However, it is too general to be applied for tracking creation of mobile money. The implementation of TLS protocol using PKI by Davies (2011) addresses data integrity using HMAC function; however, the study does not provide inputs on how TLS protocol can be used to enforce integrity, confidentiality, non-repudiation and authentication security services in tracking creation of mobile money.

The study conducted by Rwiza et al. (2020) to develop a methodology for evaluating security in MNO financial service model using insights from literature, questionnaires and interviews has implication to this study as it provides inputs for designing a secure model to track creation of mobile money. As indicated in Figure 2, there are security threats in the process of creating mobile money based on MNO financial service model (Rwiza et al. 2020).

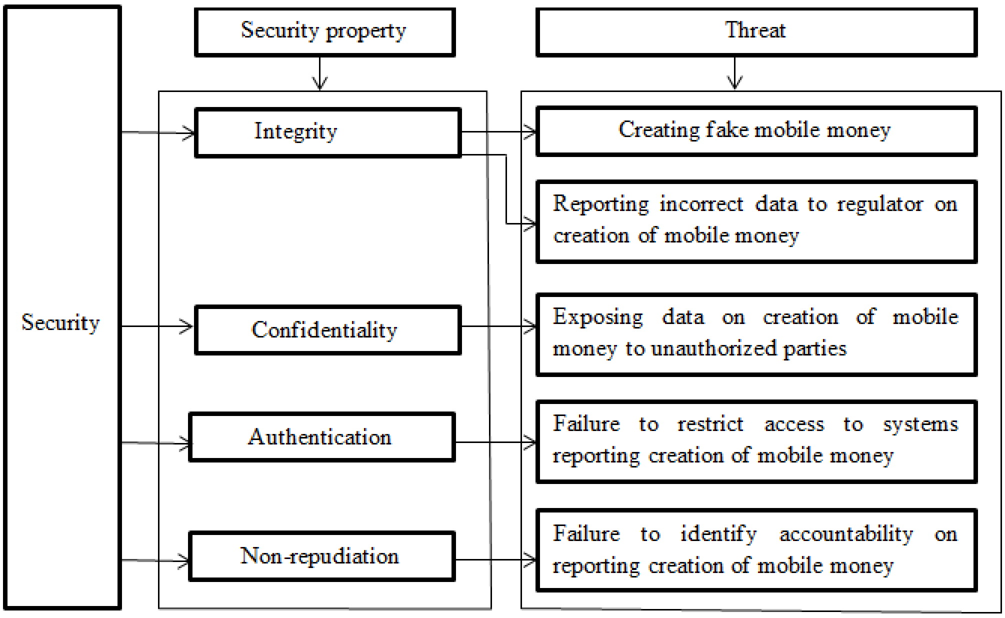

Security
Security property
Threat
Integrity
Confidentiality
Authentication
Non-repudiation
Creating fake mobile money
Reporting incorrect data to regulator on creation of mobile money
Exposing data on creation of mobile money to unauthorized parties
Failure to restrict access to systems reporting creation of mobile money
Failure to identify accountability on reporting creation of mobile money

Figure 2: Security threat model in MNO financial service model (Rwiza et al. 2020).

The security threats as summarized in Figure 2 pose challenges in tracking creation of mobile money. This leads to the need for developing a secure model to track creation of mobile money for managing risks resulting from such security threats.

Materials and Methods

Materials

This study was accomplished by using one computer on which four virtual machines were installed and configured, namely; CA, the regulator server, MNO server and bank server. As adapted from the study by Rwiza et al. (2020), the security requirements for the proposed security model were to (a) enforce integrity, confidentiality, authentication and non-repudiation security services by implementing TLS 1.3 protocol using PKI, and to (b) enforce data integrity by creating an interface for financial regulator to evaluate issued mobile money in order to detect creations of fake mobile money. In order to achieve such security requirements, there are five (5) design parameters required for designing a secure model for tracking creation of mobile money. The design parameters are trust authority (this is actually PKI system in terms of CA), parameters to monitor (returns from banks and MNOs), regulator server, bank server and MNO server.

CA is implemented for issuing, reviewing and revoking certificates and has to be owned by the financial regulator. The financial regulator has to request returns (that is, cash deposit details from banks and mobile money issuance details from MNOs) in the process of creating and issuing mobile money. The returns have to be secure by implementing TLS 1.3 protocol using PKI (in this case CA) (Hunt 2001). In the proposed model, the parameters to monitor are returns from banks and MNOs to financial regulators.

TLS 1.3 protocol has handshake protocol that provides mutual authentication services in which case regulator server and third party servers (bank and MNO servers) validate each other before data communication. TLS 1.3 protocol has record protocol using HMAC function to provide security services. The financial regulator server is used for requesting returns from banks and MNOs. It is an information retrieval tool. Financial regulator server is used to compare deposited money into trust account and issued mobile money by MNOs and stores the difference.

The bank and MNO servers are Application Programming Interface (API) servers and are implemented using Apache webserver, Laraveli PhP Framework and JSON server. These servers are accessed remotely by the financial regulator using TLS 1.3 protocol in terms of APIs (URLs). The details kept in the bank and MNO servers include amount of money deposited and amount of issued mobile money, respectively.

Developing the security model

The security model for tracking creation of mobile money using TLS protocol was developed by selecting best related security models using literature reduction process adapted from Petersen and Ali (2015). Specifications of the proposed model were obtained using function decomposition and composition processes adapted from Chiriac et al. (2011). From the four selected security models implemented using PKI, the traffic monitoring security model (Hoh et al. 2006) and the remote election monitoring security model (Kimbi and Zlotnikova 2014) were selected. The selection was based on expectations for detecting creations of fake mobile money in the country. The other criteria for selection were based on the model components relevant to the design of the proposed model. The three selection parameters were (i) trust authority (ii) the monitored parameters, and (iii) sender and receiver components. Based on traffic monitoring security model and remote election monitoring model function decomposition was applied to obtain Figure 3 and Figure 4, respectively.

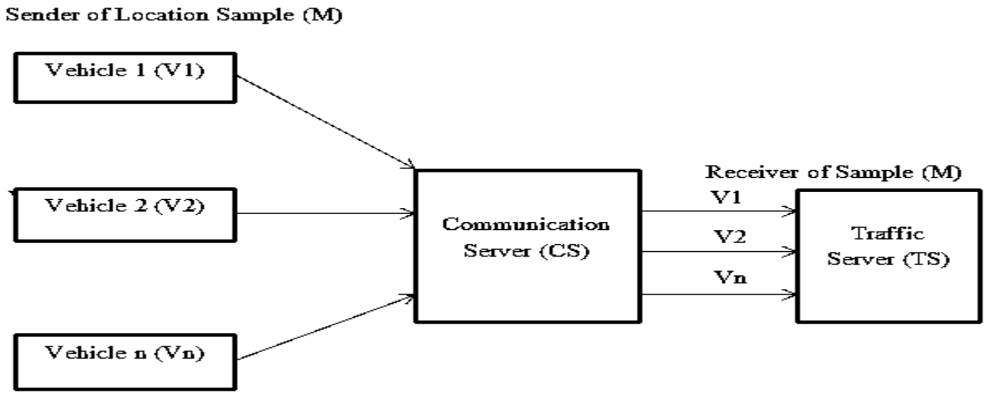


Figure 3: Function decomposition of traffic monitoring security model (Hoh et al. 2006).

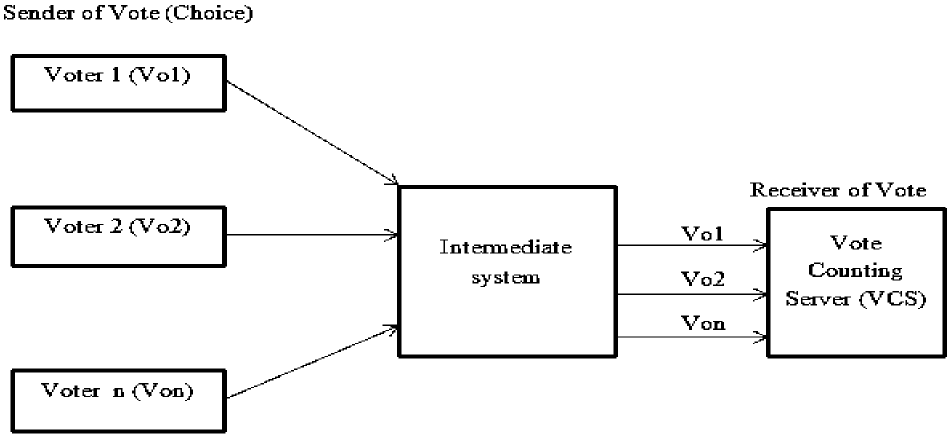


Figure 4: Function decomposition of remote election monitoring security model (Kimbi and Zlotnikova 2014).

Based on features in Figure 3 and Figure 4, function composition process was applied to obtain the architecture in Figure 5.

To implement TLS 1.3 protocol using PKI, the PKI component was added to Figure 5. The initial architecture in Figure 5 can be used to determine whether cash deposited in trust account is equal to mobile money issued by a particular MNO. However, the architecture does not guarantee security of data from banks and MNOs to the financial regulator. For instance, the financial regulator cannot ensure security of data (returns) sent by banks or MNOs and nor can the regulator validate the systems sending data to regulator system.

Hence, adding PKI system to the initial architecture resulted to the security model for tracking creation of mobile money. The detailed explanations were provided on each component for assisting system developers in applying the model to develop the system for tracking creation of mobile money. The security model for tracking creation of mobile money using TLS 1.3 protocol consists of eight components, namely; super-agent component, bank system, bank server, regulator server, PKI system, mobile money issuer component, mobile money system and MNO server.

The proposed model has been developed based on the assumption that there are non-technical security controls which include National Payment System Acts, Electronic Money Regulations, Risk Management Frameworks, Policies and Guidelines. For effective tracking of mobile money creation, there should be both technical and non-technical security measures. However, elaboration on non-technical security measures is beyond the scope of this research, and that being the case, non-technical security flaws have not been touched upon in the research.

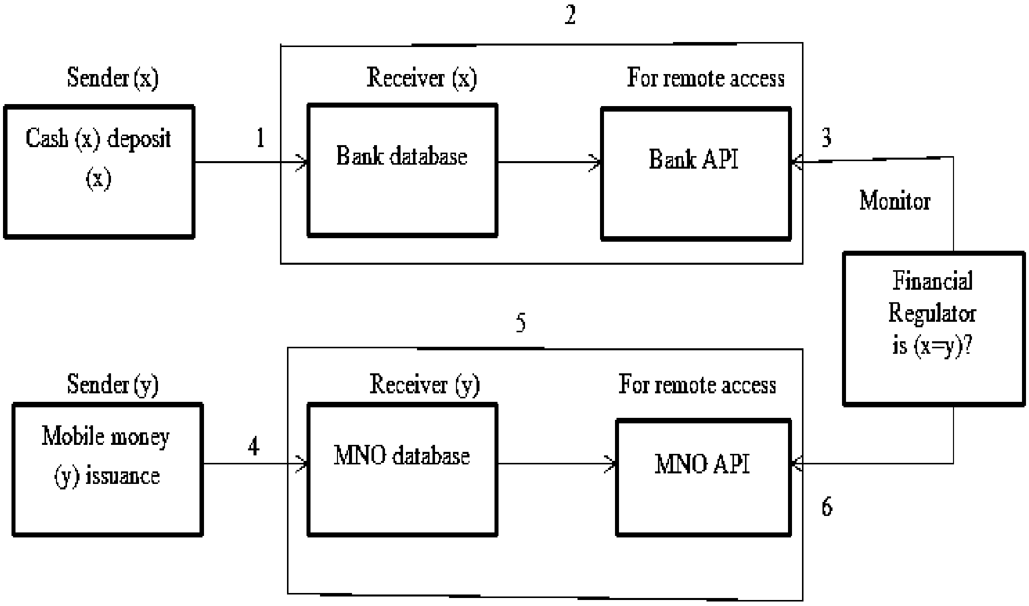


Figure 5: Initial security model for tracking creation of mobile money.

Developing the system to test the proposed model

The proposed model was in form of system architecture and related guidelines (explanations) for assisting software engineers to develop the system for tracking creation of mobile money. These guidelines are accompanied by the explanations on how the architecture would work in the real environment for tracking creation of mobile money. The first evaluation of the proposed model was to establish whether the developed model is suitable as a guideline for developing the system.

System components

The certificate authority (CA)

This was installed and configured on Windows Server 2012. The CA issues, renews and revokes certificates in the testing environment. The regulator server was installed on Windows 2010 computer, with Laravel PhP framework, apache web server and MySQL database server.

The user interface was configured using CSS3 and HTML web development languages. Certificate was installed on the server for enforcing secure (HTTPS) connections to MNO and bank servers. The Certificate Signing Request (CSR) was created using the certificates snap in the Microsoft Management Console (MMC). The CSR consisted of information explaining the identity of the owner of the certificate. The details in CA include the common name of the certificate owner, the organization, the state, the locality and the country. In creating CSR, certificate and computer account were selected and the instruction wizard was followed till the CSR was complete and saved in the computer hard disk. The CSR was then submitted to CA for requesting certificate for regulator server. CA was then configured to sign certificates. CA signed the CSR and used information carried in CSR to generate the regulator certificate.

On the regulator server, the keystore was created using keytool utility that runs on Java run time environment (JRE). The Java Netbeans development package was installed into the server which made availability of JRE facility for creating Java keystore. The certificate was then imported into the Java keystore on the regulator server on which the CSR was created. The keystore for financial regulator server consisted of the private key of the regulator server, public key of MNO server, public key of bank servers and public key of CA.

The bank and MNO servers

The bank and MNO servers were installed with apache web servers and JSON API server for allowing the financial regulator to access reports on mobile money issuance remotely. Following the same process as in regulator server, certificates for MNO and bank servers were created and installed on servers for establishing secure communication between servers using TLS 1.3 protocol.

System functions

As indicated in Figure 6, the system workflow starts with issuance of certificates by CA. These certificates are then installed into servers, namely; bank, MNO and regulator servers for enforcing authentication, integrity, confidentiality and non-repudiation security services.

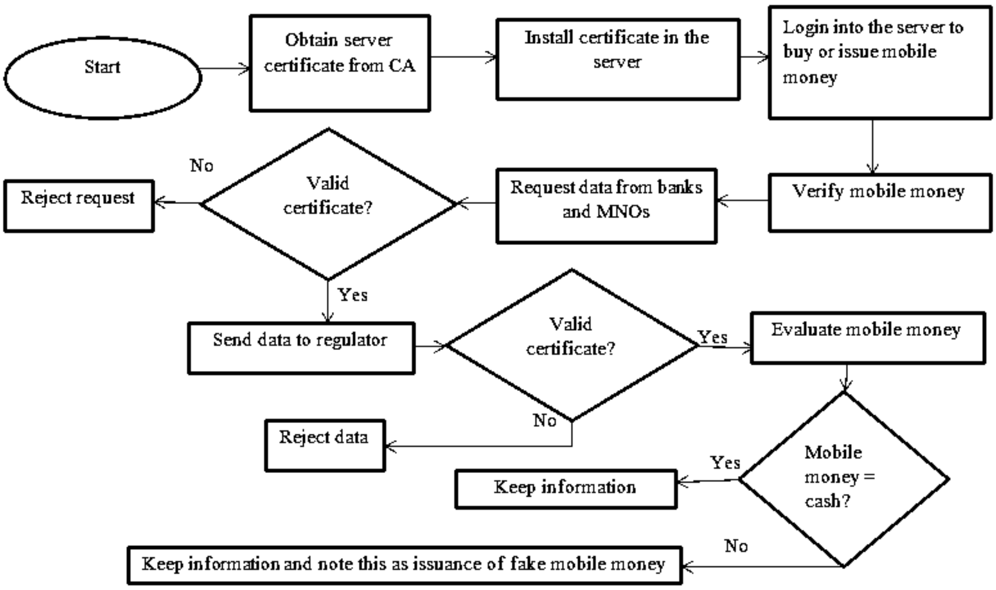
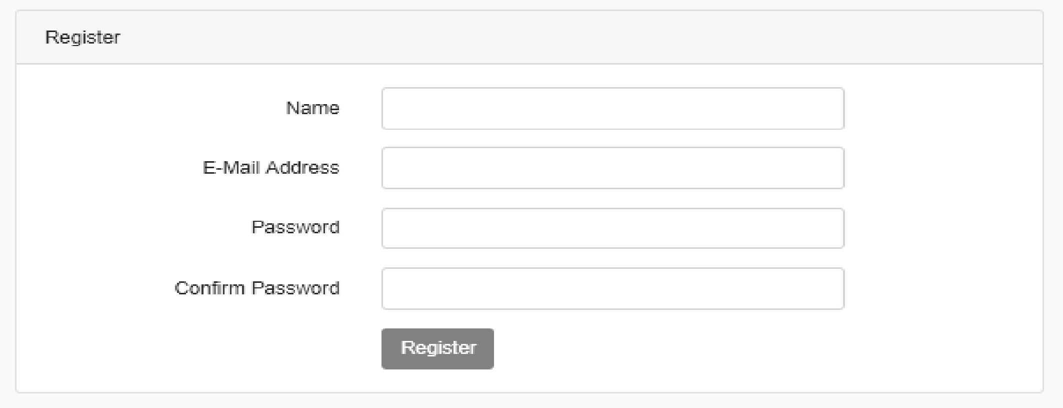

Start
Obtain server certificate from CA
Install certificate in the server
Login into the server to buy or issue mobile money
Verify mobile money
Request data from banks and MNOs
Valid certificate?
No
Reject request
Yes
Send data to regulator
Valid certificate?
Yes
Evaluate mobile money
No
Reject data
Mobile money = cash?
Yes
Keep information
No
Keep information and note this as issuance of fake mobile money

Figure 6: System flow chart showing various functions in evaluating issued mobile money.

Purchase and issuance of mobile money

The regulator application in the regulator server was used to handle verification of issued mobile money to customers (banks). For testing purposes, Laravel PhP framework, apache server and JSON server were used to configure financial regulator server, bank and MNO servers. As indicated in Figure 7, users were registered into the system by the author. The author registered each user by entering name, email address and password. Upon clicking register user details were stored into the system database.



Register

Name

E-Mail Address

Password

Confirm Password

Figure 7: Interface for logging users into the system.

Users logged into the system for different purposes. There were three categories of users, namely; (i) users buying mobile money in which case they had to deposit equivalent money into trust account; these were users from banks, (ii) users issuing mobile money to customers, these were users working in MNOs, and (iii) users evaluating issued mobile money which were from the financial regulatory sector. The users logged in using their own emails as user names and entered their passwords to proceed with system services. For testing purposes, each user was given access credentials by the author.

During data entry (that is during the process of buying and issuing mobile money), data were entered into bank and MNO systems and were moved to bank and MNO servers using JSON APIs. Financial regulator requested for data from bank and MNO servers using JSON APIs and data were carried from bank and MNO server to financial regulator using TLS 1.3 protocol in the JSON format. PhP programming language was used to enforce the functions for depositing money into trust account (bank controller), the functions for issuing mobile money (MNO controller) and the function for evaluating issued mobile money (financial regulator controller). The screen shots for buying mobile money, issuing mobile money and evaluating issued mobile money are as indicated in Figures 8, 9 and 10, respectively.

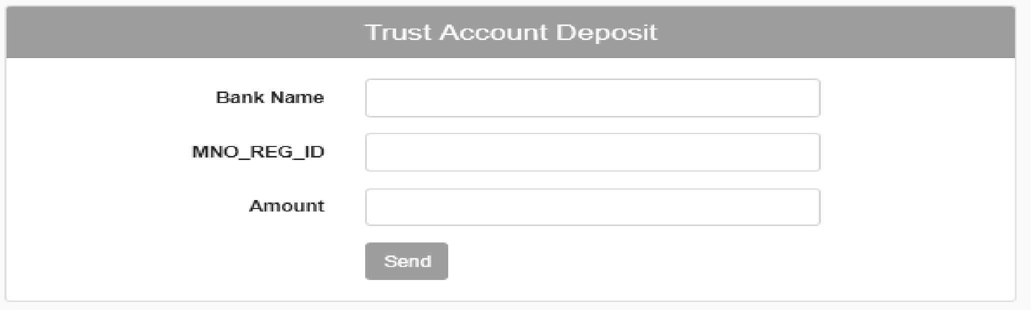


Figure 8: View for purchasing mobile money.

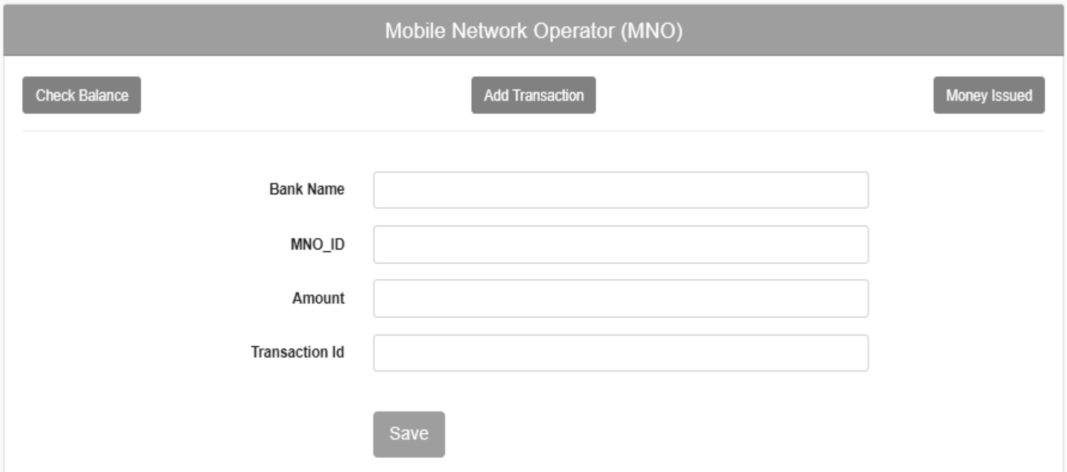
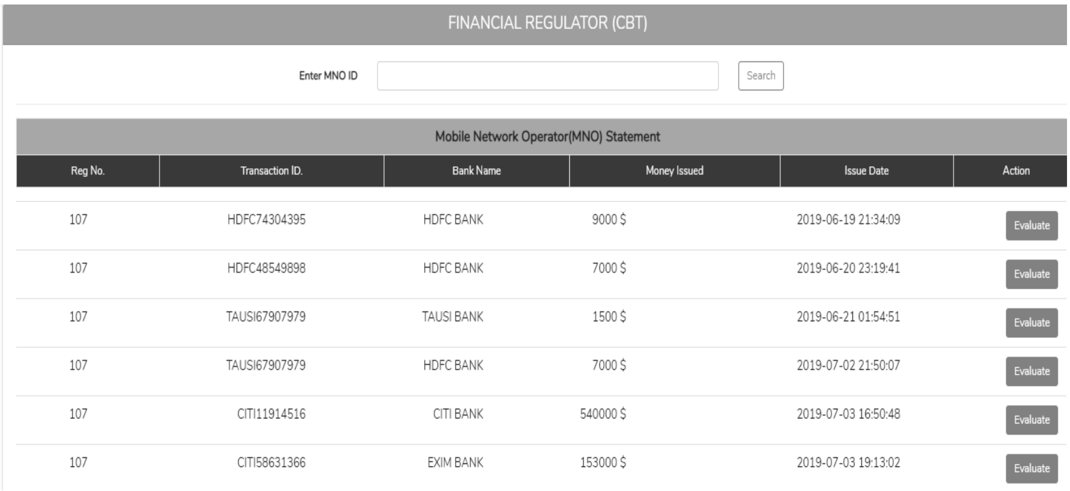


Figure 9: View for issuing mobile money.



Mobile Network Operator(MNO) Statement

Reg No.	Transaction ID.	Bank Name	Money Issued	Issue Date	Action
107	HDFC74304395	HDFC BANK	9000 $	2019-06-19 21:34:09	Evaluate
107	HDFC48549898	HDFC BANK	7000 $	2019-06-20 23:19:41	Evaluate
107	TAUSI67907979	TAUSI BANK	1500 $	2019-06-21 01:54:51	Evaluate
107	TAUSI67907979	HDFC BANK	7000 $	2019-07-02 21:50:07	Evaluate
107	CITI11914516	CITI BANK	540000 $	2019-07-03 16:50:48	Evaluate
107	CITI58631366	EXIM BANK	153000 $	2019-07-03 19:13:02	Evaluate

Figure 10: View for evaluating issuance of mobile money.

The two functions namely; purchasing and issuing mobile money take place in the systems at the bank and MNO, respectively. The variables for data entry into the system during purchase of mobile money are amount, MNO reference number, bank as the customer and the transaction ID which is generated when the details are submitted into bank system. The variables for data entry into the system during issuance of mobile money are amount of mobile money issued, MNO reference number, bank as the beneficiary of mobile money and the reference ID which is equal to the transaction ID generated during purchase of mobile money in bank system.

Evaluation of issued mobile money

During verification of issued mobile money, the regulator sends request for cash deposit details from banks. Using TLS handshake protocol, the bank server validates the regulator server and then performs hashing and encryption on the data and then sends the data to the regulator server. The regulator validates the bank server and then performs decryption and hashing processes to verify data integrity and then stores the data in its database. The regulator further requests for data from the MNO server. The same processes are done as in the bank server. The amount of cash reported by the bank is compared with the amount of mobile money reported by the MNO. If the two are equal, then the issued mobile money is verified; otherwise the issued mobile money is fake mobile money.

Evaluating the proposed model

The metric adapted from Jo et al. (2011) was used for evaluating the proposed security model. Based on judgmental sampling, fifty (50) information security evaluators were selected for evaluating the proposed model based on the metric presented in Table 1. The evaluators were given the security model for tracking creation of mobile money using TLS protocol. The model was given in terms of Figure 11 and summary explanations as presented in Figure 11. Moreover, evaluators were granted access in the system for testing the proposed model.

Ten (10) system analysts and 10 system auditors were granted access for purchasing mobile money. Ten (10) ethical hackers were granted access in the system for issuing mobile money. Ten (10) risk management officers and 10 information security officers were granted access for evaluating issued mobile money.

Evaluators used the four ranking attributes to evaluate the proposed model, namely; excellent, good, fair and poor. There were four ranking scales, namely; 1 for poor, 2 for fair, 3 for good and 4 for excellent. Responses from the 50 evaluators on ranking the integrity, non-repudiation, authentication and confidentiality security mechanisms in the proposed model based on the four ranking attributes are indicated in Table 2.

Table 1: A metric for evaluating security model implemented using PKI (Jo et al. 2011)

EC	Excellent 4	Good 3	Fair 2	Poor 1
I	PKI system is used and supports hashing algorithms for protecting data	PKI system is not used but hashing algorithms are used for protecting data	Hashing algorithm used is already broken based on literature evidence	There are no hashing algorithms used to prevent data modification
N	PKI system is used and supports use of digital signatures to achieve accountability of participating entities	There is use of digital signature to achieve non-repudiation security mechanism but not based on PKI system	Digital signatures are not used but some other non-repudiation security mechanisms are used	There is no use of non-repudiation security mechanisms at all
A	There is use of PKI system that supports validation of systems before exchanging information	PKI system is used but does not support validation of systems before exchanging information	PKI system is not used but there are other authentication security mechanisms used	There are no authentication security mechanisms used at all
C	PKI system is used and provides encryption algorithms for preventing data exposure	PKI system is used but explanation is not provided on how it achieves encryption to prevent data exposure	PKI is not used but some other confidentiality security mechanisms are used.	There are no encryption algorithms used for protecting data exposure.

In Table 1, EC represents evaluation criteria, I, N, A and C represent integrity, non-repudiation, authentication and confidentiality, respectively.

Table 2: Evaluation of the proposed model using selected metric

S/N	Evaluated security service (EC)	Percentage of respondents for each ranking attribute			
		Excellent	Good	Fair	Poo
1.	Integrity	70	8	22	0
2.	Non-repudiation	60	36	4	0
3.	Authentication	86	10	4	0
4.	Confidentiality	56	24	20	0

Seventy percent (70%) of the evaluators reported that in the proposed model, integrity security mechanisms are excellent in the sense that the PKI system is used in which case integrity was achieved using HMAC function and SHA-3 context as presented in the explanation to the architecture for the secure model. HMAC functions are implemented in combination with hashing algorithm context to achieve authenticity and integrity of data (Davies 2011). In this study, SHA-3 context was used with the HMAC function to achieve data integrity. However, 22% reported that integrity security mechanisms are just fair; this was probably due to the fact that they were not very much aware on the use of HMAC function to enforce integrity security service in PKI systems.

Eighty six (86%) of the evaluators reported that there is use of PKI system and explanation is provided on how it supports validation of systems before exchanging information. Such evaluators were probably very much aware on how servers exchange certificates in the handshake protocol for validating each other. Furthermore, sixty (60%) of the evaluators reported that PKI system is used and supports excellent use of digital signatures to achieve accountability of participating entities. Moreover, 56% of the evaluators reported that PKI system is used and provides excellent encryption algorithms for preventing data exposure. Such evaluators were aware of the strength of Rivest, Shamir and Addleman (RSA) asymmetric algorithm as the encryption algorithm used in the proposed model and the decryption algorithm with bit length of 2048 for private key used in the proposed model.

Results and Discussion

As indicated in Figure 11, the security model for tracking creation of mobile money using TLS 1.3 protocol consists of eight components, namely; super-agent, bank system, bank server, regulator server, mobile money issuer, mobile money system, MNO server and CA (referred to as PKI system). The process labeled 8 in Figure 11 is the process for implementing TLS protocol using PKI; PKI (in this study) refers to CA and its related services for issuing, revoking and renewing certificates. Hence, in this study CA was installed and configured for issuing, renewing and revoking certificates. The owner of CA should be a trusted authority; hence financial regulator was identified as the trusted authority in tracking creation of mobile money and was selected as the owner of CA.

The regulator has to develop the server and install the certificate issued by CA in the server. The regulator server is then configured to send HTTPs requests to banks and MNO servers using TLS protocol. This makes enforcement of authentication, integrity, confidentiality and non-repudiation security services. Likewise, banks and MNOs have to develop API servers in which they allow the regulator to view data remotely using APIs (URLs). Implementation for remote data access is done using REST API and transfer of data is done using JSON format along HTTPS (TLS) protocol.

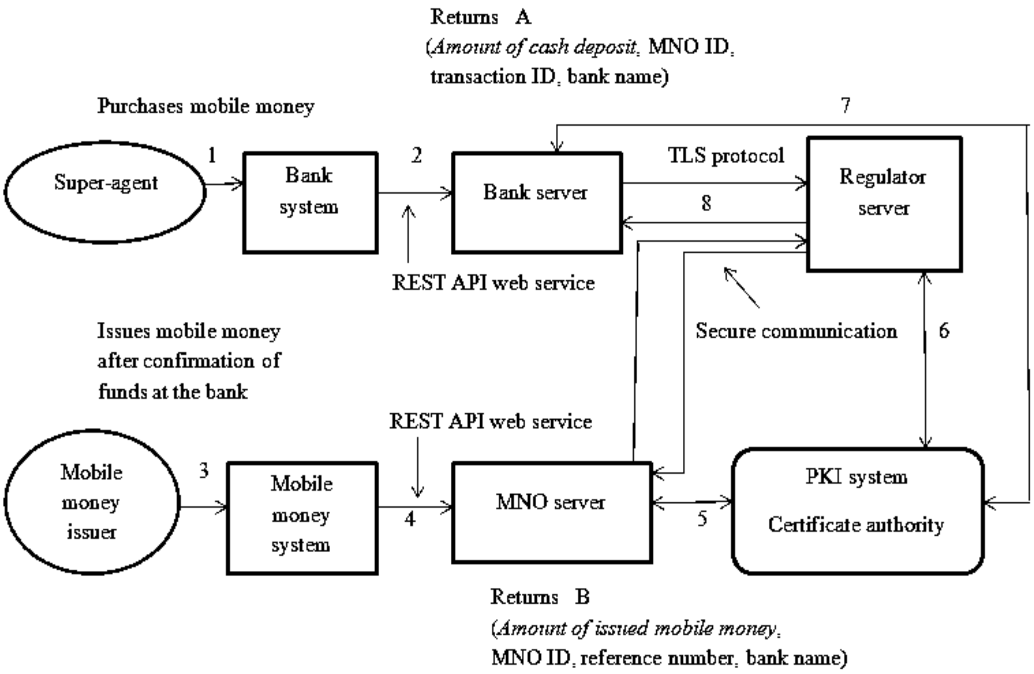


Figure 11: Security model for tracking creation of mobile money using TLS protocol.

At bank and MNO environment, software engineers have to install certificates issued by CA in their servers. Each certificate is installed in the server in form of keystores and contains private key of the server, public key of other servers and the public key of CA. The TLS protocol has handshake protocol and record protocol.

The security model for tracking creation of mobile money using TLS 1.3 protocol has eight processes. The tracking of creation of mobile money starts from step 1 up to step 8. However, since the financial regulator does not have direct access to the banking system and mobile money system, the actual tracking of creation of mobile money is based on returns A and B at bank and MNO servers, respectively. What is tracked is the amount of mobile money issued by mobile money issuer and the amount of money deposited by the super-agent in the trust account of mobile money issuer.

The essence for tracking creation of mobile money is to confirm whether the amount of issued mobile money is equal to the amount of money deposited by the super-agent at the bank. To avoid duplicate issuance of mobile money for the same cash deposit, the transaction ID generated during the crediting of the trust account of mobile money issuer should be equal to the reference number involved in issuing mobile money to super-agent.

In the process labeled 1, the super-agent logins into the bank system and purchases mobile money by depositing money in the trust account of the mobile money issuer at the bank. In depositing money into the trust account, the MNO account is credited and relevant details are recorded in bank system, namely; amount of cash deposit, MNO ID, transaction ID and bank name. The super-agent uses the web application interface to credit the trust account.

In the step labeled 2, using Representation State Transfer (REST) API web service the details referred to as returns A are made available in the bank server which is actually bank API server. The returns referred to as A consist of amount of deposited cash in trust account, account of MNO referred to as MNO ID, transaction ID and name of the super-agent (bank) depositing money into trust account. In this case, it is the name of the super-agent.

In the step labeled 3, the mobile money issuer logins into mobile money system and issues mobile money to the super-agent after confirmation of availability of money in the trust account. In the step labeled 4, using REST API web service the details referred to as returns B are made available in the MNO server which is actually MNO API server. The returns referred to as B consist of amount of issued mobile money, issuer of mobile money (MNO ID), reference number and name of the super-agent issued with mobile money. In this case, it is the name of the bank issued with mobile money.

In the process labeled 5, the mobile money issuer requests for certificate from CA; CA issues the certificate and then mobile money issuer installs the certificate into MNO server in form of keystore consisting of private key of MNO server, public key of financial regulator server, public key of CA. At any time, MNO (mobile money issuer) may request for certificates, verify certificates and request a revocation of certificates. Hence, the communication between the MNO server and the CA should be two way communications as indicated in Figure 11.

In the process labeled 6, financial regulator requests for certificate from CA; CA issues the certificate and then financial regulator installs the certificate into financial regulator server in form of keystore consisting of private key of financial regulator server, public key of bank server, public key of CA and public key of MNO server. At any time, financial regulator may request for certificates, verify certificates and request a revocation of certificates. Hence, the communication between financial regulator server and the CA should be a two-way communication.

In the process labeled 7, bank registered as super-agent in mobile money services requests for certificate from CA; CA issues the certificate and then the bank installs the certificate into bank server in form of keystore consisting of private key of bank server, public key of financial regulator server and public key of CA. At any time, the bank may request for certificates, verify certificates, and request a revocation of certificates, request for public keys of other entities and the like. Hence, the communication between bank server and CA should be a two-way communication.

The communication between third party server (bank or MNO server) and financial regulator server is across the internet. The process labeled 8 indicates configuration of TLS 1.3 protocol to establish secure communication channel across the internet. The secure communication channel consists of TLS handshake protocol and record protocol. In the handshake protocol, communication is established and returns A and B are transmitted during the record protocol. Hence, in the process labeled 8, financial regulator server requests for returns from the bank or MNO server. In order to achieve authentication security service, the handshake protocol enables servers to exchange certificates. The bank or MNO server verifies the certificate of the regulator server by comparing with the public key of the server on the certificate and that installed in its server; if the two match, then the regulator server is validated by the bank or MNO server.

Data communication takes place in the record protocol. In order to achieve data integrity security service, the returns A or B are passed through HMAC function, the digest from the HMAC function is signed using the private key of the sender (bank or MNO server) and the original data are encrypted using the public key of the regulator server. The encrypted message

(MSG) and the signed digest (TAG) are sent to the regulator server. The regulator server verifies the signed digest using public key of the sender (whether bank or MNO server). The financial regulator server decrypts the cipher text (MSG) using its private key and turns the plain text into hash value using HMAC function. If the two digests are equal, then returns A or B from bank or MNO server along the communication channel were not modified while in transit.

In the processes labeled 8, confidentiality is achieved using asymmetric encryption. This happens by encrypting the returns A or B with the public key of the regulator server. At the receiver part, the regulator server decrypts the cipher text (MSG) using its private key. The Rivest, Shamir and Adleman (RSA) encryption algorithm is used and the private key used in servers has 2048 bits. The data is thus known and seen by the bank or MNO server and the regulator server. Unauthorized parties cannot have access to the data.

To achieve non-repudiation security service, the digest sent to regulator server is signed using private key of the sender (whether bank or MNO server). The regulator server verifies the signature of the bank or MNO server using public key of sending server (be it bank or MNO server). Hence, with such kind of digital signature, the bank or MNO server cannot deny of having sent returns to financial regulator. The financial regulator tracks creation of mobile money based on such returns A and B from bank and MNO servers, respectively. Moreover, at the beginning of the communication, the bank or MNO server and regulator server validate each other; in that case authentication security service is achieved using handshake protocol. The data from banks and MNOs to financial regulators are just small bytes in which case public key encryption may be used. However, for bigger data additional hardware components known as Peripheral Component Interconnect (PCI) can be added on server motherboards for improving speed of the financial regulator server while maintaining security efficiency.

Conclusion

As summarized in Figure 11, various parameters have been covered in the proposed model, namely; financial regulator server (for tracking issued mobile money), PKI system (CA) (for being used by the TLS protocol to form a secure communication channel along which returns (data) from banks and MNOs are carried to financial regulators) and tracked returns (the basis for financial regulators in tracking creation of mobile money).

The paper contributes to the body of knowledge a security model for racking creation of mobile money using TLS protocol. Specifically, the paper contributes four parameters to the body of knowledge, namely: implementation of TLS protocol using PKI for assisting financial regulators to track creation of mobile money, returns from banks and MNOs for tracking creation of mobile money, system architecture for tracking creation of mobile money and prototyping of the system for tracking creation of mobile money.

Conflicting of Interest

Authors declare that no conflict of interest exists.

Acknowledgements

The Central Bank of Tanzania deserves fervent gratitude for sponsoring this research out of which this work came into existence. Secondly, we are very grateful to the College of Information and Communication Technologies (CoICT) at the University of Dar es Salaam for providing technical review and guidance in conducting this research.

References

Al-Janabi S and Obaid AK 2012 Development of certificate authority services for web applications. *International Conference on Future*

Communication Networks. ICFCN *2012*. January: 135–140.

Castri SD and Gidvani L 2014 Enabling mobile money policies in Tanzania. *GSMA*. February: 1–13.

Chiriac N, Hölttä-Otto K, Lysy D and Suh ES 2011 Three approaches to complex system decomposition. *Invest on Visualization-Proceedings of the 13th International DSM Conference*. January 2011: 3–17.

Curguz J 2016 Vulnerabilities of the SSL/TLS protocol. *Computer Science & Information Technology*, 245–256.

Davies J 2011 Implementing SSL/TLS Using Cryprography and PKI. John Wiley and Sons Inc.

Hoh B, Gruteser M, Xiong H and Alrabady A 2006 Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*. November*:* 38-46.

Houmani H and Debbabi M 2012 Formal analysis of the TLS handshake protocol. *Proceedings of the International Conference on Security and Cryptography*. SECRYPT-2012: 192–205.

Hunt R 2001 PKI and digital certification infrastructure. *Proceedings of Ninth IEEE International Conference on Networks.* ICON: 234–239.

Jo H, Kim S and Won D 2011 Advanced information security management evaluation system. *KSII Transactions on Internet and Information Systems* 5(6): 1192–1213.

Kimbi S and Zlotnikova I 2014 A secure model for remote electronic voting: A case of Tanzania. *Adv. Comput. Sci. Int. J.* 3(4): 95–106.

Latif MK, Jacinto HS, Daoud L and Rafla N 2018 Optimization of a quantum-secure sponge-based hash message authentication protocol. *2018 IEEE 61st International Midwest Symposium on Circuits and Systems.* MWSCAS: 984–987.

Misra S, Goswami S, Taneja C, Mukherjee A and Obaidat MS 2015 A PKI adapted model for secure information dissemination in industrial control and automation 6LoWPANs. *IEEE Access.* 3: 875–889.

Nyamtiga B, Anael S and Loserian L 2013 Enhanced security model for mobile banking systems in Tanzania. *Int. J. Technol. Enhance. Emerege. Eng. Res.* 1 (4): 4–20.

Petersen K and Ali NB 2015 Operationalizing the requirements selection process with study selection procedures from systematic literature reviews. *CEUR Workshop Proceedings* 1342: 102–113.

Rwiza S, Kissaka M and Kapis K 2020 A methodology for evaluating security in MNO financial service model. *IST-Africa 2020 Conference Proceedings* 905824-65-6: 1–10.

Toapanta M, Nazareno J, Tingo R, Mendoza F, Orizaga A and Mafla E 2018 Analysis of the appropriate security models to apply in a distributed architecture. *IOP Conf. Ser.: Mater. Sci. Eng.* 423(1): 012165.

Zhao G and Chadwick DW 2008 On the modeling of Bell-LaPadula security policies using RBAC. *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises.* WETICE: pp. 257-262.