Available online at www.rajournals.in

RA JOURNAL OF APPLIED RESEARCH
ISSN: 2394-6709
DOI:10.47191/rajar/v10i08.04
Volume: 10 Issue: 08 August-2024

International Open Access

Impact Factor- 8.174

Page no.- 204-218

Secure Mobile Money Withdraw Framework – SeMWiF

Job Matovu[1], Drake Patrick Mirembe[2], Odongo Steven Eyobu[3]
[1,2,3]College of Computing and Information Sciences, Makerere University.

ARTICLE INFO

Published Online:
21 August 2024

ABSTRACT

Financial and Data loss from Weak withdrawer Authentication in Mobile Money is a heavy burden to individuals, organizations and governments. To reduce this burden, an easy to use and acceptable secure mobile money withdraw framework should be designed that can detect, prevent and assist in recovery of fraudulent mobile money withdraws. To achieve this, the study had three study contributions; Studying different Mobile Payment withdraw frameworks; Designing a secure Mobile Money withdraw framework and; Evaluating the usability and usefulness of the designed secure Mobile Money withdraw framework. This paper presents the Secure Mobile Money Withdraw Framework (SeMWiF), a new software construction, that detects, prevents and assist in recovery of fraudulent mobile money withdraws. Evaluation results show that, SeMWiF enhances Detection, Prevention and Recovery, with an Ease of Learning rating at 51%, Ease of Use rating at 71% and Perception of Acceptance at 71 % as well. Should the Secure Mobile Money Withdraw Framework-SeMWiF guidelines be implemented, Mobile Money stakeholders will experience greater use from enhanced security and less financial loss.

Corresponding Author:
Job Matovu

KEYWORDS: Mobile Payment Systems, authentication Attacks, Mobile Security.

I. BACKGROUND OF MOBILE PAYMENT SYSTEMS

Mobile payment systems have grown worldwide for example Africa's mobile payment industry has grown significantly however, this growth in the low digital literacy environment (Junior, et al., 2023) has also led to an increase in financial loss. According to Uganda Police annual crime report, in 2021 Ugandan banks had lost over $4 million to hackers in 2020 and there was an increase in cybercrime from 256 cases reported to police in 2020 to 286 cases reported in 2022, giving a 10.8% increase (Aine, 2023). According to a report from the Criminal Investigative Directorate (CID), Shs 5 billion was carelessly sent to 877 AIRTEL SIM cards, while Shs 5.5 billion was sent to MTN SIM cards (Arinda, 2023).

Mobile Money services were blocked in Uganda for days in 2016 due to national security reasons and the government was sued for property, livelihoods and consumer rights connected to mobile money transactions like financial losses suffered and criminal money transfer. Criminals use mobile payments to transfer money for drug trafficking, stolen vehicles, illegal firearms, and counterfeit pharmaceuticals that cause 500,000 deaths every year in Africa alone (Jerving, 2023; UNODC report., 2023). Additionally, criminals can easily access personal information from government or business websites, such as names, dates of birth, ID numbers, and telephones, to open fake mobile money accounts and load them with illegal money. This has led to cases of kidnapping, extortion, and ransom demands, with mobile money being the expected mode of payment (INTERPOL, 2020; Monitor., 2021).

Some of the approaches being used to improve authentication in Uganda include; employing security guards at mobile money agent's premises and operating during working hours. Setting up burglar proof kiosks and better still to build the kiosks similar to a mini-bank branch. Requiring any form of identification like a National, school ID or passport. Money reversals by some service providers like MTN Uganda has a USSD service reversal which is *165*8*7# (Guma, et al., 2020). These approaches are not focused on improving withdrawer authentication and as a result even when in place, an impersonator can still take money from the system with weak authentication.

Financial loss and criminal money transfer are attributed to the poor authentication in the withdraw transactions that attach no or weak physical identity to the withdrawer inspiring this study to design a secure mobile money withdraw framework. The study therefore sought to design a secure mobile money withdraw framework, with these guiding study contributions;

1. A review of different Mobile Payment withdraw frameworks
2. A design of a secure Mobile Money withdraw framework
3. An evaluation of the usability and usefulness of the designed secure Mobile Money withdraw framework

The rest of the paper is organized as follows; Section 2 Related works, section 3 the methodology, Section 4 discusses the study results and section 5 presents the conclusions and recommendations.

II. RELATED WORKS

A. Mobile Money Crime

Globally, the cost of cybercrime was predicted to hit $8 trillion in 2023 and will grow up to $10.5 trillion by 2025 (eSentire Inc, 2023). Africa's mobile payment industry has grown significantly, with 469 million Mobile Money users making $456.3 billion transactions annually and an estimated 66% mobile penetration by 2025. However, this growth in the low digital literacy environment (Junior, et al., 2023) has also led to an increase in financial loss, with Africa recording $5 billion in mobile payment financial losses annually (Lepecq, 2020; Gilbert, 2021; Kanali, 2021)

Table 1: Showing the Extent of Mobile Crime.

	Mobile Penetration	**Extent of Mobile Crime**
Global	6.92 billion which is 85.95% global phone ownership (Ash, 2023) 5.4 billion mobile money transactions (Guma, 2022)	The cost of cybercrime was predicted to hit $8 trillion in 2023 and will grow up to $10.5 trillion by 2025 (eSentire Inc, 2023).
Africa	1.4 billion people in Africa, 621 million mobile money accounts (Guma, 2022)	Total transaction value grew by 22% between 2021 and 2022 in Sub-Saharan Africa First five months of 2023, there were 764,015 detections of malicious files aimed at phones in Middle East, Turkey and Africa (Parker, 2023). 469 million registered mobile money accounts generating $456.3 billion in transactions from 2019 (Africa's mobile money industry is infiltrated by crime. (n.d.)
Uganda	30.55 million own a mobile phone (Kemp, 2023). $31.9 billion mobile money transactions value (Guma, 2022)	6,936 phones reported stolen UPF Annal crime report 2022. 43.6 billion stolen in 2022 206 incidents of fraud were reported in 2022. Serugo, 2023

In Kenya where Mobile money started, a user registers for the MoMo service through the MNO's mobile application, websites, Unstructured Supplementary Service Data (USSD), call centers or agents. Registration requirements include; a SIM card from a licensed MNO and their original identity card. An agent registers new users and these users must securely enter a PIN number. That is confidential and only known to the user. The virtual money is always in the customer's control. Therefore, there is no credit risk to either the customer or the MNO (Admin., 2020b).

Kenya however has reported a high incidence of financial loss, with 47.4% of users reporting such incidents, including sending money to the wrong number which was not returned or recovered through authorities. In Uganda, 60% of users reported suffering from financial loss in 2017 (Guguyu, 2021; Buku & Mazer, 2017). According to Uganda Police's annual crime report, in 2021 Ugandan banks had lost over $4 million to hackers in 2020 and there was an increase in cybercrime from 256 cases reported to police in 2020 to 286 cases reported in 2022, giving a 10.8% increase (Aine, 2023). According to a report from the Criminal Investigative Directorate (CID), Shs 5 billion was carelessly sent to 877 AIRTEL SIM cards, while Shs 5.5 billion was sent to MTN SIM cards (Arinda, 2023). Table 1.2 shows mobile related crime from 2009 to 2022.

The use of mobile payments for criminal activities is also a significant concern. Mobile Money services were blocked for days in 2016 due to national security reasons and the government was sued for property, livelihoods and consumer rights connected to mobile money transactions like financial losses suffered and criminal money transfer. Criminals use mobile payments to transfer money for drug trafficking, stolen vehicles, illegal firearms, and counterfeit pharmaceuticals that cause 500,000 deaths every year in Africa alone (Jerving, 2023; UNODC report., 2023). Additionally, criminals can easily access personal information from government or business websites, such as

names, dates of birth, ID numbers, and telephones, to open fake mobile money accounts and load them with illegal money. This has led to cases of kidnapping, extortion, and ransom demands, with mobile money being the expected mode of payment (INTERPOL, 2020; Monitor., 2021).

Table 2: Mobile Money related crime in Uganda

Source	Uganda Police Force (UPF) Annual Crime Reports - Phones Stolen	Mobile Money Theft	Reference
2009	15,264		UPF Annual Crime Report 2009.
2010	11,908		UPF Annual Crime Report 2010.
2011	6,812	MTN lost Ugx 21 B MTN lost Ugx 16 B	UPF Annual Crime Report 2011. Mousal, 2015. Independent, 2017
2012		MTN lost $ 3.5M	UPF Annual Crime Report 2012. Finextra., 2012
2013	4,409	MTN lost Ugx 3.1 B	UPF Annual Crime Report 2013. MTN staff, cleaner and mobile money agent get 9 years for fraud, 2021b
2015	210		UPF Annual Crime Report 2015.
2016	106		UPF Annual Crime Report 2016.
2017	158	67B stolen	UPF Annual Crime Report 2017. Telecoms, bank hacked, over sh1b stolen. (n.d.-b)
2018	6,205		UPF Annual Crime Report 2018.
2019	5,630	More than Ugx 41 B	UPF Annual Crime Report 2019. Kafeero, 2022.
2020	4,043	$ 3.2 M (MTN and Airtel suspended mobile transactions) Ugx 1 B	UPF Annual Crime Report 2020. Kafeero, 2022. Aheebwa, 2022
2021	4143		UPF Annual Crime Report 2021
2022	6,936	Ugx 19 B	UPF Annual Crime Report 2022 Understanding cybercrime in Uganda., 2024

Financial loss and criminal money transfer are attributed to the poor authentication in the withdraw transactions that attach no or weak physical identity to the withdrawer inspiring this study to seek for better ways to improve the withdrawer-authentication in mobile money system.

B. Types of Mobile Money Fraud

***Impersonation Fraud*:** Impersonation fraud takes two forms, one being social engineering and the other identity theft as seen in the next exposition. Social Engineering Fraud; fraudsters involve unsuspecting victims, influencing them to open mobile money accounts to profit from government's economically empowering programs like the Parish Development Model (PDM). After opening these accounts, account owners surrender their Personal Information to fraudsters remember this is all a con, for a fee. Working closely with staff at mobile money service providers centers, the fraudsters are able to identify idle accounts holding large sums of money (Aine, 2023). Identity Theft Fraud; Identity theft-criminals easily access personal information from government or business websites like Names, Dates of birth, ID numbers and telephones. Criminals use Attack Points on different components of the MM Service, which they then use to open up fake mobile money accounts and load them with illegal money, kidnapping, extortion as in 2019 an American tourist kidnapped in Uganda and in 2020 a Chinese national kidnapped in Kenya and in both cases mobile money was the expected mode of payment (INTERPOL, 2020).

***Insider Fraud*:** Insider fraud takes three forms, one being embezzlement, corruption then data theft and system breach. Embezzlement Fraud takes two forms, fictitious electronic values and theft of physical cash is reported in forms of armed robberies and in some cases, deaths (Aine, 2023), have been reported by the police, when theft of mobile money was taking place. Money is not only stolen from customers but agents and service providers as well. As examples, in 2015, MTN lost 10 billion Uganda shillings (Waswa, & Waswa, 2017). Robbers monitor the schedules of mobile money users like the time they close and open their shops. Upon getting a clear picture of agent's or

customer's movements and the roads used, they rob mobile money users. In the face of resistance, mobile money users are killed. Sometimes robbers pretend to withdraw huge sums of money like in millions from mobile money agents, intending to find out if the agent has a lot of cash at hand. While making transactions, criminals may pretend to have forgotten their PIN or telephone number and go away after getting the evidence wanted about the amounts of cash kept around. Later they organize other robbers to commit crime (Zurah, 2016; Arafat, 2022). Corruption Fraud through bribery and extortion, where some employees of mobile money providers, agents or organizations actually plan with robbers by disclosing pin numbers for their mobile money accounts. Then robbers attack, robbing phones and withdraw cash quickly (Zurah, 2016; Arafat, 2022). Insider incidents within mobile payment provider organizations are often witnessed in the media. These insider incidents maybe happening in addition to other causes like blackmail, corruption, foolery (social engineering) and corruption but whichever way, "Money is lost and even when criminals are arrested, the money is not returned" – a statement from one of the respondents. Staff within provider organizations, team up with criminals to carryout illegal activities like financial loss and data loss (Humphrey, 2018; Joseph, 2018). In 2016 fake mobile money float was created with 21 billion Uganda shillings within MTN through insider incidents, in 2019 again MTN lost 100 million Uganda shillings through insider incidents and in 2022, 30 billion Uganda Shillings was reported stolen from Airtel (Charles, 2019; Christine, 2019; Elizabeth, 2020).

Cyber Fraud: This takes the forms of Man-in-the middle, Denial of Service (DoS) and Malwares. Man-in-the middle Fraud an example is threats or Gifts from Telecom staff or those pretending to be telecom staff. Anonymous callers to random numbers with threats like closing a Sim card line due to some sort of customer non-compliance with the service provider. As mentioned above, unknown people will call, claiming to be telecom company staff or even offering employment opportunities. However, to access all these fake services, one has to share their mobile money PIN code (Mudiri, 2013).

Agent Fraud: Commission arbitrage, Illegal fees and services and Confidentiality breaches. Confidentiality breach Fraud Reading numbers loudly breaches confidentiality. This is one of the growing tricks in mobile money theft. "Ochan Michael narrated how he was robbed. He innocently approached a mobile money operator to withdraw money on his MTN line. He went ahead and did all the procedures, inserted the pin, and later received a message confirming the transaction. On asking for his money from the agent, he said he did not withdraw the money. Confused, Ochan showed him a message confirming the transaction, but the agent insisted he had not withdrawn any money from him. After a few minutes of shock, one of the agents nearby said that someone else had withdrawn the money. As Ochan was reading his number, someone else was initiating, and so when he inserted the pin code, the money was transferred to the fraudster instead" (Mudiri, 2013; Arinda, 2023).

KYC breaches Fraud: Commission arbitrage, Illegal fees and services and Confidentiality breaches. KYC breaches Fraud; Poor customer identification; Weak-Withdrawer Authentication is another security challenge in Mobile Payment Systems. The Weak-Withdrawer Authentication is the single factor of authentication (4-digit code used in plain text), Attaches no Physical Identity to withdrawer, as a result we witness financial loss, Data loss and Threats to users (Buku & Mazer, 2017). Financial loss; Governments lose money that should support the state and citizens, Business lose money that should support business processes and profits, Individuals lose money that should support personal developments. Fear of transacting with mobile payment systems results in a search for alternative payment methods like cash and yet mobile payment systems should be embraced because they provide most benefits of physical cash at a reduced cost and with more productivity (Dahlberg, 2015), what mobile payment systems should provide is reduced cost, increased productivity and security that physical cash does not do.

***Cash-in-Cash-out Fraud*:** Where quick float is needed, a request for transfer of float (electronic money) is sent to an agent-A who will receive a phone call from someone pretending to be a fellow mobile money agent (agent-B) and yet this caller is indeed a fraudster. They will go ahead and describe a former transaction the agent-B did together with agent-A and rush Agent-A into sending the float in the name of "Agent-B has a customer – and quick float is needed for a transaction", by the time the agent-A realizes they have been scammed it is too late.

C. Mobile Money Withdraw Fraud Mitigation Approaches

Mtaho 2015, observed that the use of PIN as authentication method is vulnerable to illegal Mobile Money Services access. To address this problem, a 2FA model that uses PIN and fingerprint recognition technology was proposed. The study proposed the use of two-factor authentication model that combines the current approach of using PIN and adds another layer of security that uses fingerprint recognition technology. The study did not do the cost benefit analysis of the proposed model. This study assumed that the proposed model will work with smartphones (which have embedded fingerprint recognition technology) some phones do not support biometric features, creating a need to study how the proposed model can be applied to basic mobile phones.

Chetalam, 2018, developed an android platform model - VMPESA, in response to issues regarding implementing a secure mobile-based multi-factor authentication scheme using device specific ID, voice biometric and a PIN for

securing MPESA transactions. The study concluded PIN is not a sufficient security measure when performing mobile transactions and fraudsters are taking advantage of this vulnerability to defraud MPESA subscribers by using techniques such as SIM-swap, reversal transactions and scam messages. Voice biometrics is a factor that can enhance authentication with specific reference to MPESA mobile money transfer system. The study recommended that for mobile money service providers should concentrate on implementing multi-factor authentication schemes in their system. They should also identify the major weaknesses of the implementing single factor authentication, such as PIN, as a security measure. Mobile money service providers should also be aware that fraudsters are employing new techniques everyday therefore continuous upgrade of the security features is imperative. Safeguarding subscriber personal information and account is extremely important and should be top priority to these organizations. The study did not explore alternative multifactor authentication schemes which have more functionalities to make the entire process more seamless, convenient for the subscribers and intelligent in nature. The study did not identify advanced techniques used by fraudsters to acquire subscribers' personal information.

Islam et al., 2019 proposed a money transfer system to enhance the security of payment process for SMEs in Bangladesh. To attain this objective, a conceptual framework from an Industry 4.0 perspective along with required algorithm is proposed that uses iris verification technique to authenticate a user uniquely. The study focused on iris-based authentication approach to enrich the security of mobile financial service for SMEs in Bangladesh in order to reach the era of Industry 4.0 for achieving better productivity, reliability, and customer satisfaction less developed industries are out of this technical scope. The proposed system does not store iris of the user because of privacy concerns. So, the user must provide iris for each transaction. Again, the system requires to connect with national data server for matching the biometric measures against the NID number.

Ranyali 2019, The study proposed a conceptual framework that mitigates security vulnerability introduced by the current method of authentication in Mobile Money (PIN), with multi-factor authentication using Biometric Face Recognition (BFR) technique. BFR eliminates the chances of a fraudster providing false information to the system, therefore improving the security of the system. Further research is needed on how to enhance the security in face recognition system, through its algorithms and machine learning. This study did not focus on different frauds techniques that are used to steal subscriber's money and models that Mobile Network Operators in Lesotho can use to detect and minimize fraud in M-money.

Mega 2020, This study proposed a framework to improve security the usage of Mobile Money Services by using two-factor authentication (2FA) of PIN and iris biometric authentication method in Tanzania. designing the framework to improve security level in accessing Mobile Money Services based on iris recognition biometric authentication method - IRBAM. The proposed 2FA framework of PIN and iris biometric authentication method proved to remove unauthorized access to Mobile Money Services. The study focused on implementing biometric authentication on smartphones - feature phones were left out of scope. The study did not focus on implementing liveness detection mechanism on iris recognition on accessing MMS thus imposters may get access to the services.

Chebii, 2021 developed a mobile application - SAFECASH that analyses and holds un confirmed transactions, blacklists suspended contacts and locks suspected transactions against social engineering attacks (smishing and vishing) in mobile money. This study was limited to social engineering attacks (smishing and vishing) in mobile money. The study focused on social engineering risk in mobile money transactions. Another limitation is that SAFECASH does not authenticate calls and SMS.

Sanni et al., 2023, The study observes that traditional security techniques are too broad to address increasing and widespread mobile cybercrimes to Mobile Financial Services (MFS). The existing body of knowledge is not adequate for predicting threats associated with the mobile money ecosystem. Thus, a need for an effective analytical model based on intelligent software defense mechanisms to detect and prevent these cyber threats. Through this study, a dataset was collected via interview with the mobile money practitioners, and a Synthetic Minority Oversampling Technique (SMOTE) was applied to handle the class imbalance problem. A predictive model to detect and prevent suspicious customers with cyber threat potential during the onboarding process for MMS in developing nations using a Machine Learning (ML) technique was developed and evaluated. This study focused on mobile phone subscriber biodata registration details for Mobile Money Services. Other components of the customer lifecycle management process such as modification (SIM SWAP), customer biometrics, profile modification and customer termination processes as cyber threat vectors for MMS were not explored.

D. Mobile Money Withdraw Fraud Mitigation Approaches in Uganda

Bopape 2015, The study developed a unified fraud management and digital forensic framework to improve the security of mobile phone applications. This proposed unified approach to fraud management and digital forensic, simultaneously manages and investigates fraud that occurs through the use of mobile phone applications. The unified Fraud Management and Digital Forensic (FMDF)

framework is designed to (a) determine the suspicious degree of fraudulent transactions and (b) at the same time, to feed into a process that facilitates the investigation of incidents. The study was limited to South African environment, a presence in other countries could be useful. Enhanced use can be got from focus on industries other than the financial services industry, which was the primary focus of this study, testing applicability with experts in those fields. Since fraud management and digital forensics is not limited to mobile applications, there is need to investigate the use of the approach for next-generation communication platforms. The study did not model nor operationalize the proposed framework. There is need of modelling the framework and designing a dedicated system architecture to operationalize the framework in a real-life setting.

Nzayinambaho 2021, The study designed a multifactor authentication security model, an additional layer of security to improve on the transaction security used in mobile banking system, to improve the security system using a multifactor authentication security model for AB Bank Rwanda. The developed model offers remedy to challenges faced by mobile banking users in AB Bank by offering them another way of authorization and authentication after putting in PIN to approve transactions, which reduces theft and other related threats that result from inadequate security mechanisms in place. Clients were not taught about strong protection for their accounts by creating passwords that are difficult for hackers to replicate and use to scam mobile banking customers. The study did not investigate additional aspects that enhance online banking security, only USSD Push was explored, upcoming scholars may study the other aspects that contribute to improved online banking security in financial institutions. Further research on the use of iris recognition, biometrics, voice recognition and Artificial Intelligence to assist in reducing frauds that may arise in the available security mechanisms.

Adedoyin 2018, The ability of Mobile Money Transfer services (MMT) to handle large number of small value payments worldwide funds exchange in digital currencies and lack of oversight makes it an attractive target for attackers and fraudsters. Although the risks inherent in all payments channels exist in the mobile money payment environment. The usage of mobile money transfer technologies introduces additional risks caused by the large number of non-bank participants, higher speed of transactions and level of anonymity compared to mobile banking and mobile commerce systems. This study proposed a pattern recognition model to predict fraud in Mobile money transfer transactions. The study did not build an improved model or a more realistic dataset using a combination of synthetic and real data. This would make it even more valuable as a realistic dataset for fraud detection experiments.

Guma, 2022 This study focused on developing a secure multi-factor authentication (MFA) algorithm for mobile money applications. To authenticate and authorize mobile money subscribers, personal identification numbers, one-time passwords, biometric fingerprints, and quick response codes are used. Secure hash algorithm-256, Rivest-Shamir-Adleman encryption and Fernet encryption were used to secure the authentication factors, confidential financial information and data before transmission to the remote databases. The study designed a secure MFA algorithm for mobile money applications and developed three native G-MoMo applications to implement the designed algorithm to prove the feasibility of the algorithm and that it provided robust security. The algorithm was resilient to non-repudiation, ensured strong authentication security, data confidentiality, integrity, privacy, and user anonymity, was highly effective against several attacks but had high communication overhead and computational costs. The G-MoMo applications' interface designs lack forward navigation buttons, uniformity in the applications' menu titles, search fields, actions needed for recovery help and documentation.

Table 3: SeMWiF and Other Mobile Money Withdraw Mitigation Approaches

	Name	Framework	Authentication	Model	Reference
1	2FA Model		PIN + Finger print		Mtaho 2015
2	Fraud Management and Digital Forensic - FMDF			Detection And prevention	Bopape, 2015
3	V-Mpesa		Voice biometric (1FA)		Chetalam, 2018
4	Pattern Recognition Model			predicts fraud	Adedoyin, 2018
5	Secure MM Transfer System		Iris Biometric (1FA)		Islam et al., 2019
6	Biometric Face Recognition -BFR		-digit encrypted PIN + Face Biometric (2FA)		Ranyali et al., 2019

7	Iris Recognition Biometric Method - IRBM	Security	PIN + Iris Biometric (2FA)		Mega 2020
8	SAFECASH		Email and password + Private ID and Telephone Number (1FA)	Analyses copies of everything we are shifting. Blacklists suspected contacts. Lock suspected accounts	Chebii, 2021
9	MFA security model		PIN + USSD push token [device ID and IMEI] – (2FA)		Nzayinambaho, 2021.
10	Secure MFA application		PIN + Token (QR) + Thumb Biometric (3FA)		Guma, 2022
11	Predictive cyber-threat Model			Detective and Preventive	Sanni et al., 2023
12	SeMWiF	Security	PIN (encrypted) + Token (NFC) + Face Biometric (3FA)	Detects, Prevents and Recovery	

The literature clearly shows that the current practice of securing Mobile Money withdraw transactions with a PIN is weak and attaches no physical identity to the withdrawer consequently impersonators continue to take money from the Mobile Money system. To be secure, Mobile Money withdraw transactions should have Detection, Prevention and Recovery Schemes (Shirey, 2000; Stallings & Brown, 2012; Wu & Meng, 2018). None of the reviewed security approaches to mobile money withdraw provide a solution that has detection, prevention and recovery schemes with a multifactor authentication approach that attaches physical identity to the withdrawer. There is therefore a need to enhance Mobile Money withdraw security through multifactor authentication, that attaches physical identity to the withdrawer. This therefore inspired this study to design a secure mobile money withdraw framework – SeMWiF that has detective, preventive and recovery schemes.

III. METHODOLOGY

A qualitative research approach to data collection and analysis was adopted. Respondents to this study were selected using a purposive sampling technique (Cochran, 2007; Mirembe, et al., 2019), they included; Mobile Money Agents, Mobile Money Customers, and Security Experts from Uganda. Respondents were selected based on their unique qualities that made them likely to provide the desired opinions and experiences about the use of mobile payment systems in Uganda (Mirembe, et al., 2019). A security expert was defined as an individual with over 10 years of experience in; research, designing and developing security systems especially financial systems, had a minimal of master's degree in Computer Science or related fields with a bias on cyber security. A total of 14 participants responded to the study, out of which 9 were male and 5 were female. The participants included 2 PhD holders, 4 PhD candidates, 1 Financial Technology Developer, 3 mobile money agents and 4 mobile money customers.

IV. THE SECURE MOBILE MONEY WITHDRAW FRAMEWORK-SEMWIF

A. Secure Mobile Money Withdraw Framework-SeMWiF

The Mobile Money withdraw transactions are protected by three security mechanisms; the first security mechanism which is Detective (Device Proximity), then they are protected by the second mechanism which is Preventive (Multi-Factor Authentication) and by a third mechanism which is Corrective (Recovery with Transaction Reversal). This study conceptualizes that for Mobile Money Systems to be secure in the Secure Mobile Money Withdraw Framework - SeMWiF, they need to make Detections of money withdraw transaction attacks and Preventions of money withdraw transaction attacks and Recoveries from money withdraw transaction attacks in the event that the detections and preventions failed. The attackers include malicious people, amateur hackers, cyber criminals, compromised employees among other. The defenders include customers, agents, regulators and the governments working with mobile money systems.

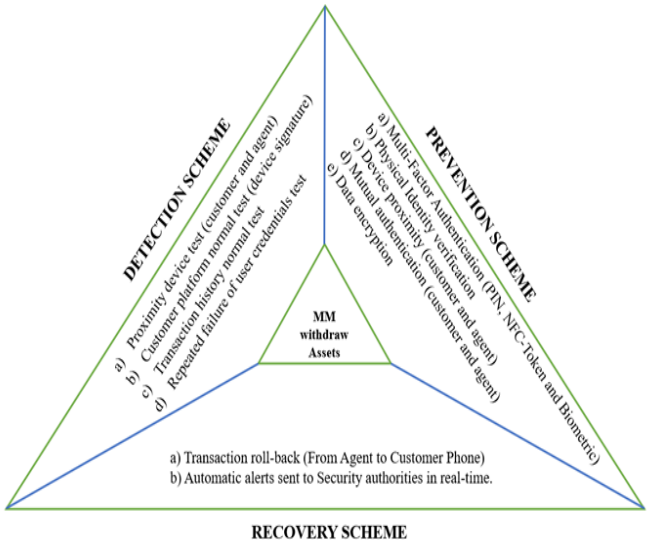

Figure 1: Secure Mobile Money Withdraw Framework – SeMWiF

The Secure Mobile Money Withdraw Framework – SeMWiF, has 3 components which are the Detection, the Prevention and The Recovery, with various SeMWiF Security Metrics like;

Proximity

Using Near-Field Communication (NFC) for proximity test. Sophisticated NFC tags can execute code, hold operating systems and many complex interactions (Ahamad, 2021; Zhou, et al., 2022). All mobile money users (customers and agents) to have NFC enabled devices that can exchange data with peer NFC devices. Any money withdraw transaction in which the agent and customer devices are not within a maximum of 4cm should be is rejected.

Device Signature

Capturing device specific details at mobile money account creation. These details include; details from *197*4# (phone type, among others), details from *#06# (IMEI), national identity (National Identity Card, Passport or school Identity Number). Then all consecutive mobile money transactions can be recognized with valid and up-to-date secure cash withdraw transactions.

Transaction History

Details of concern may include; withdraw amounts, source of funds and purpose of funds. These details are profiled for mobile money accounts and they keep growing, then mobile money withdraw transactions become easier to cross-check before allowing secure mobile money withdraw transactions. For example, the study makes some assumptions the following rules:

1. Any transaction above 5,000,000 is suspicious
2. Any transaction made between 10 PM and 6AM is suspicious
3. Any transaction made from a location other than the user's usual locations is suspicious. Otherwise, the money withdraw is rejected or put on hold for investigation.

Repeated Failure

Any 3 or more than 3 consecutives withdraw fails may need to be watched closely for brute force attacks, social engineering and their variations. The money withdraw is rejected or put on hold for investigation.

Three Factor Authentication

MM service providers need to integrate Multi-Factor Authentication to enhance security of MM withdraw transactions, and this can be represented mathematically (Lampson et al., 1992; Bouchet, et al., 2020);

Knowledge Factor: PIN(P) and Security Question (Q): Kf = {P, Q}

Possession Factor: NFC-Token (N) using a shared secret (S): Pf = {N, S}

Biometric Factor: Face Verification (F): Bf ={F}

The Mobile Money multi-factor authentication withdraw transaction is represented mathematically in a formula as follows:

Authentication= {▉ (MM Withdraw accepted if "Kf" is valid and "Pf" is valid and "Bf" is valid@Otherwise MM Withdraw denied) ┤

As a result, three factors of authentication are a requirement at the mobile money withdraw. Otherwise, the money withdraw is rejected.

Agent-Customer Authentication

The customer and agent are physically at the same place, and thus symmetric key cryptography is very helpful which - shares a secret key between two parties a sender and a receiver who wish to communicate securely without revealing details of the message. The secret key is used for both encryption and decryption of the message (Isaac & Sherali, 2014; Srinivas et al., 2019). All mobile money users (customers and agents) are to have NFC enabled devices that can exchange data with peer NFC devices.

Server-Client Authentication

Asymmetric cryptography is good at providing non-repudiation, authentication and securing short message services. Common public key protocols include, SSL/TLS, SSH, IPSec and SET among others while algorithms used include Rivest Shamir and Adelman - RSA and Elliptic Curve Cryptography-ECC, Diffie-Hellman and ElGamal among others (Pukkasenung & Chokngamwong, 2016; Chaudhry et al., 2017). As a result, public key cryptography is a requirement at the mobile money withdraw and any money withdraw transaction.

Malicious Transaction Roll-Back

User transaction reversal (roll-back) - mobile money users need to be empowered to make withdraw transactions reversals by themselves but with monitoring from the security teams, so as not to abuse the empowerment. Then SeMWIF monitors the roll-backs using a confusion matrix. This is helpful as long as the money has not been withdrawn however in case the money has been withdrawn, then

Automatic alerts become helpful. An example of a Mobile Money Transaction roll-back can have output as;

True Positive: a successful identification of stolen MM at withdraw transaction

True Negative: ignoring a legal MM Withdraw transaction.

False Positive: fake threat or non-malicious MM withdraw transaction.

False Negative: a MM withdraw transaction threat that did not trigger.

SeMWIF quarantines devices and users who are True Positive: a successful identification of stolen MM at withdraw transaction, for future reference.

Automatic alerts to security teams.

In the event that the Mobile money has been already been withdrawn, it is really hard to return the stolen money. However, SeMWIF proposes the Automation of SMS alerts to security personnel. An example of a Mobile Money alert confusion matrix can have output as;

True Positive: a successful transmission of MM alert to security team.

True Negative: ignoring a legal transmission of MM alert to security team.

False Positive: fake threat or non-malicious transmission of MM alert to security team.

False Negative: a MM alert to security team that did not trigger.

Automatic alerts to security personnel when a misused account should issue an alarm to the Judiciary, the Telcom company and Police. At the expense of the misused account. With an SMS costing Ugx 50/=, it would cost an account Ugx 150/= for these alerts each time. SeMWIF quarantines devices and users who are True Positive: a successful transmission of MM alert to security team.

Table 4: SeMWIF outlier Detection, Prevention and Recovery.

Security Scheme		Test	Security Metric	Outlier Output		Security Goal
			Threshold	Normal	Abnormal	
Detection	1	Proximity	4cm Or Less			Confidentiality Integrity Authorization Accountability Non-Repudiation
	2	Device Signature	Valid Mm Device And User Details			Integrity
	3	Transaction History	Participation In Mm Related Crime			Confidentiality Integrity
	4	Repeated Failure	More Than 3 Consecutive Mm Withdraw Fails.			Availability
Prevention	5	3fa	Availability And Validity Of Authentication Factors			Authentication Authorization Accountability Non-Repudiation
	6	Agent-Customer Device Authentication	Availability And Validity Of Authentication Factors			Confidentiality Integrity Authorization
	7	Server-Client Authentication	Availability And Validity Of Authentication Factors			Confidentiality Integrity Authorization
Recovery	8	Transaction Roll-Back	Failed And Successful Roll-Backs			Availability Accountability Non-Repudiation
	9	Automatic Fraud Alerts.	Failed And Successful Alerts			Availability Accountability Non-Repudiation

Mobile Money Withdraw Process

The Secure Mobile Money Withdraw Framework-SeMWiF mobile money withdraw process can be seen in about 6 steps as;

1. The customer presents a cash withdraw request to the agent with withdraw details like the telephone number and amount to be withdrawn.

b. In some cases, the agent asks the customer to initiate the money transfer from the server.

c. following 1b. above, the customer then initiates a money transfer from the customer's phone through the server.

d. The server sends the customer a secret code.

e. customer shares secret code with agent, who proceeds to make a money request from the server as in step 2. (Note: steps b, c, d and e are simply an alternative)

2. The agent then initiates a money transfer from the customer's phone to the agent's phone through the server.

3. SeMWiF has a Detection Component before sending a multifactor authentication request approving mobile money transfer.

4. The server after getting the transfer request from the agent sends a PIN authentication request to the customer's device.

5. SeMWiF has a Prevention Component for the multifactor authentication response approving mobile money transfer from the customer.

6. Customer responds by submitting the multifactor authentication, done using agent's device for customer's with feature phones – these feature phones must have an NFC sticker or tag that the agent smartphone reads. however, if the customer has a smartphone, they can submit these multifactor authentication responses from their phone.

The Multifactor Authentication factors include;

a) The NFC Proximity test picked by the server (agent and customer)

b) Customer face scan

c) Token (Valid Identity Card– that was used at Mobile money account opening)

d) PIN (not used in plain text)

7. SeMWiF has a Recovery Component for the mobile money transfer from the customer to the agent. This is a transaction reversal.

8. The server then makes the transfer from the customer's phone to that of the agent.

9. After the agent has got the money on their mobile money account, they give a cash equivalent to the customer and the withdraw transaction is completed.

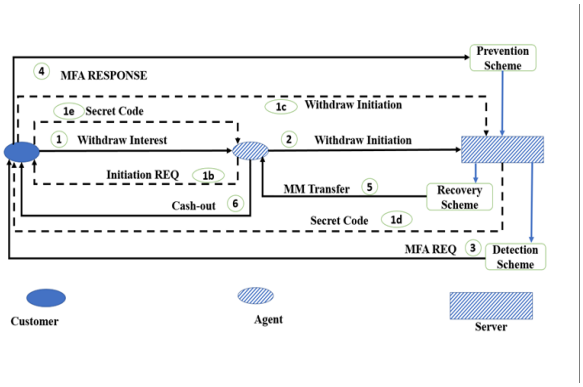

Figure 2: SeMWiF Mobile Money Withdraw Process

B. To evaluate the usability and usefulness of the designed Secure Mobile Money Withdraw Framework

Evaluation of Secure Mobile Money Withdraw Framework – SeMWiF, was done to establish that the designed artefact (SeMWiF) enhances mobile money withdrawer authentication through usefulness and usability measurements. Perceived usefulness and usability are good parameters for evaluation as derived from the Technology Acceptance Model. This evaluation was done by users who were into two categories – mobile money System Experts and Users (Agents and Customers). Mobile money users and security Experts were given questionnaires in order for them to participate in these evaluations. The evaluation procedure followed; 1. A paper-based evaluation which iterated until a stable version was got. 2. Instantiation of the artefact, implementing SeMWiF into a consumable product, and 3. Parallel SeMWiF evaluation between experts and users.

Evaluation Procedures: Evaluators of the Secure Mobile Money Withdraw Framework - SeMWiF were purposively selected, based on their unique qualities that made them likely to provide the desired opinions and experiences about the use of mobile payment systems in Uganda (Cochran, 2007; Mirembe, et al., 2019), they included; Mobile Money Agents, Mobile Money Customers, and Security Experts from Uganda. A security expert was defined as an individual with over 10 years of experience in; research, designing and developing security systems especially financial systems, the expert also had a minimal of master's degree in Computer Science or related fields with a bias on cyber security. The experts were drawn from; Academia (3) and FinTech systems developer (1). The users were Mobile Money Agents (3), Mobile Money Customers (7).

Table 5: General Information from respondents.

	Qualification	Number	Evaluator's Role
1	Doctorate	2	Security Experts
2	Master's Degree	1	
		1	Systems Developer
		3	Customers
3	Bachelor's Degree	2	Agents
		2	Customers

4	Diploma /Certificate	2	Customers
		1	Agents
	Total	**14**	

Evaluation Method: Evaluation provides evidence that a developed artefact serves the purpose it was designed and developed. In order to accomplish study objectives, response was collected from evaluation, defining appropriate parameters from which opinions and subsequently conclusions be made (Mirembe, 2015). A mixed methods research approach involving qualitative and quantitative methods of data collection and analysis was adopted. The evaluation of the Secure Mobile Money Withdraw Framework – SeMWiF involved two steps which were; 1. The Paper-based evaluation, which led to the Instantiation of Secure Mobile Money Withdraw Framework - SeMWiF into a consumable service this was followed by 2. Parallel evaluation of Secure Mobile Money Withdraw Framework – SeMWiF between experts and users.

Likert Scale Evaluation Tool: The study used Linkert scales which were named after their inventor, psychologist Rensis Likert, in the evaluation of the Secure Mobile Money Withdraw Framework - SeMWiF. Linkert scales are a type of rating scale used in surveys and questionnaires to measure attitudes, opinions, and perceptions of individuals or groups towards various topics, to measure and compare attitudes and opinions across individuals or groups, and they are widely used in fields such as psychology, social sciences, marketing, and education. This study used 5-point Likert-type question with five response alternatives (Strongly Agree - SA, Agree - A, Not Sure – NS, Disagree - D and Strongly Disagree - SD) to determine the usefulness and usability of the Secure Mobile Money Withdraw Framework – SeMWiF (Tumwebaze, 2016; Namatovu, 2018).

Testing: Expert Walkthrough Evaluation Exercises**.** The Evaluation exercise on the Usefulness and usability of SeMWiF involved mobile systems experts who are researchers at Makerere University currently doing their PhD in a computer related course.

Usefulness Evaluation of SeMWiF application results

Table 6: Evaluation on the Usefulness of SeMWiF

Evaluation Questions	SA	A	NS	D	SD
1. The SeMWiF application is useful in detecting malicious activities in Mobile Money transactions?	66%	33%			
2. Multi-Factor Authentication in the SeMWiF application is useful in preventing malicious activities in Mobile Money transactions?	66%	33%			
3. Mixed Data Replication is useful in recovering lost data in Mobile Money transactions?		100%			

The Evaluation exercise on the Usefulness of SeMWiF also inquired from the respondents about the vulnerabilities that are currently identified in the SeMWiF application and the responses are below.

Table 7: Vulnerabilities and additional features which may be missing in SeMWiF

Other Evaluation Questions	Responses
1. Are there any vulnerabilities that you have identified in using SeMWiF application for malicious activities detection in Mobile Money transactions?	• No vulnerabilities • No vulnerabilities • The NFC beaming in very fast and yet some customers may be slow in entering the data.
2. Are there any vulnerabilities that you have identified in using Multi-Factor Authentication for malicious activities prevention in Mobile Money transactions?	• No vulnerabilities • Some people do not want their faces used in other people's phones. • No vulnerabilities
3. How well does the SeMWiF integrate with other systems and technologies within the Mobile Money ecosystem?	• Currently no integration • Through registration and accessing data in the eco-system • The system can integrate very well in the eco-system
4. Are there any additional features or capabilities that you believe could be added to the SeMWiF to improve its usefulness?	• Auto photo capture by agent's phone • Extending the service to mobile money related systems like in banking • The study should add Finger print biometrics

Usability Evaluation of SeMWiF application results

Table 8: Usability Evaluation results of SeMWiF

Evaluation Questions	SA	A	NS	D	SD
1. Users can easily understand the security features (multi-factors of authentication) of SeMWiF?	33%	33%		33%	
2. Users can easily enable and disable SeMWiF security features when needed?		100%			
3. Security interfaces of the SeMWiF are familiar?	33%	33%		33%	
4. The language used in SeMWiF security notifications and alerts is clear?	66%	33%			
5. The security features of the SeMWiF (multi-factors of authentication), are helpful?	66%	33%			
6. The security features of the SeMWiF (multi-factors of authentication), are annoying?				66%	33%

The Evaluation exercise on the Usefulness of SeMWiF also inquired from the respondents about the vulnerabilities that are currently identified in the SeMWiF application and the responses are below. User Experience Testing and Evaluation (Customers and Agents)

The Usability evaluation of the SeMWiF application from customers and agents of mobile money Using a 5-point Linkert scale, the SeMWiF prototype was tested as follows, Strongly Agree – SA, agree – A, Not Sure – NS, Disagree - D and Strongly Disagree-SD.

Usability Evaluation of SeMWiF application

Table 9: Barriers to continued use and other key issues which the study may have left out

Evaluation Questions	SA	A	NS	D	SD
1. It feels comfortable when entering personal information in the SeMWiF app?	29%	29%	43%		
2. It was difficult to create a secure account on the SeMWiF app?		29%		57%	14%
3. It was easy to understand the security features (multi-factors of authentication) of SeMWiF app?	14%	86%			
4. It was easy to enable and disable SeMWiF app security features when needed?		57%	29%	14%	
5. Security interfaces of the SeMWiF app are familiar?	14%	43%	43%		
6. The language used in SeMWiF app security notifications and alerts is clear?	14%	71%	14%		
7. The security features of the SeMWiF app (multi-factors of authentication), are helpful?	29%	57%	14%		
8. The security features of the SeMWiF app (multi-factors of authentication), are annoying?				57%	43%
9. Would you recommend the SeMWiF app for friends and family when making mobile money withdraws?	14%	71%	14%		
10. At the moment nothing can prevent me from using the SeMWiF app for money withdraw?		57%	43%		

Mobile Money user engagement during SeMWiF evaluation, with a Mobile Money customer on the left and a Mobile Money agent on the right.

C. Evaluation of Results

The study used percentages as a method to represent data, showing the frequency with which categories of data occur. The relative frequency being the percentage of observations within a given category (Viray, 2016).

f=N*n/100……. Eqn 1.1

Where;

f-Frequency

N-Total number of respondents

n- Percentage of occurrence

Table 10: Usability Evaluation Results

	Parameters	Percentages
Usability	1. Learnability	86%
	2. Annoying	33%
	3. Ease of use	57%
	1. Satisfaction	71%
	2. Efficiency in execution	66%

The Secure Mobile Money Withdraw Framework - SeMWiF application is easy to learn and in general users are satisfied with the application. The study revealed that the use of Multi-factor Authentication to improves overall identity management and system security. The study also revealed that majority of respondents 66% agreed that the designed SeMWiF is useful in detecting, preventing and making recovery from mobile money withdraw attacks.

V. CONCLUSIONS AND FUTURE WORK

All paragraphs must be indented as well as justified, i.e. both left-justified and right-justified. The study results show that, the great reliance on a single factor of authentication is major contributor to insecurity in mobile money transactions and the use of Multi-factor Authentication to improves overall identity management and system security. The study has increased the Security awareness of mobile money risks especially in the withdraw transactions, with all the participants as respondents (customers, agents and evaluators), software developers, experts in fintech and the banking sectors, seminar participants like PhD weekly seminars at Makerere and other research platforms like ESCANET among others. Should the Secure Mobile Money Withdraw Framework-SeMWiF guidelines be implemented, mobile money stakeholders will experience greater use from enhanced security and less financial loss.

VI. ACKNOWLEDGEMENTS

This study would like to extend warm appreciation to ESCANET Research Group members. Your contributions are priceless and may GOD reward you richly. In a special way, the study wishes to recognize the efforts by, The College of Computing and Information Sciences at Makerere University – COCIS.

REFERENCES

1. Adedoyin, A. (2018). Predicting fraud in mobile money transfer (Doctoral dissertation, University of Brighton).
2. Africa's mobile money industry is infiltrated by crime. (n.d.). Cash Essentials. https://cashessentials.org/africas-mobile-money-industry-is-infiltrated-by-crime/
3. Aheebwa, J. (2022, June 28). How Ugandans lose millions in mobile money fraud. Monitor. https://www.monitor.co.ug/uganda/business/prosper/how-ugandans-lose-millions-in-mobile-money-fraud-3862312
4. Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717-723.
5. Ali, Guma, Ally Dida, M., & Elikana Sam, A. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. Future Internet, 12(10), 160.
6. Arinda, C. (2023, May 19). TRICKS USED BY MOBILE MONEY FRAUDSTERS IN UGANDA. Nexus Media. https://nexusmedia.ug/tricks-used-by-mobile-money-fraudsters-in-uganda/
7. Bopape, R. K. (2015). Towards a Unified Fraud Management and Digital Forensic Framework for Mobile Applications (Doctoral dissertation, University of South Africa).
8. Bouchet, M., Cook, B., Cutler, B., Druzkina, A., Gacek, A., Hadarean, L., ... & Warfield, A. (2020, November). Block public access: trust safety verification of access control policies. In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (pp. 281-291).
9. Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2016). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electronic Commerce Research, 16(1), 113-139.
10. Chebii, P. J. (2021). Securing Mobile Money Payment and Transfer Applications Against Smishing and Vishing Social Engineering Attacks (Doctoral dissertation, University of Nairobi).
11. Chetalam, L. J. (2018). Enhancing Security of Mpesa Transactions by Use of Voice Biometrics (Doctoral dissertation, United States International University-Africa).

12. Cochran, W. G. (2007). Sampling techniques. John Wiley & Sons.
13. eSentire Inc. (2023, October 28). Cybersecurity Ventures report on cybercrime. eSentire. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on cybercrime#:~:text=The%202023%20Cybersecurity%20Ventures%20Cybercrime%20Report%20predicts%20a%20rapid%20increase,%243%20trillion%20recorded%20in%202015.
14. Finextra. (2012, May 28). Ugandan telco says employees stole $3.5m in mobile money fraud. Finextra Research. https://www.finextra.com/newsarticle/23759/ugandan-telco-says-employees-stole-35m-in-mobile-money-fraud
15. Guillaume Lepecq (2020). Africa's Mobile Money Industry is Infiltrated by Crime. From https://cashessentials.org/africas-mobile-money-industry-is-infiltrated-by-crime/ on 16 May 2022 at 8:19am
16. Guma, A. (2022). Development of a secure multi-factor authentication algorithm for mobile money applications (Doctoral dissertation, NM-AIST).
17. Independent. (2017, January 15). Inside MTN mobile money saga. The Independent Uganda: https://www.independent.co.ug/inside-mtn-mobile-money-saga/
18. INTERPOL, Project ENACT: Mobile money and organized crime in Africa, June 2020. This analytical report was compiled in the framework of the European Union (EU) funded Project ENACT (Enhancing Africa's response to transnational organized crime). The contents of this INTERPOL report can in no way be taken to reflect the views of the EU or the ENACT partnership.
19. Isaac, J. T., & Sherali, Z. (2014). Secure mobile payment systems. IT Professional, 16(3), 36-43.
20. Islam, I., Munim, K. M., Islam, M. N., & Karim, M. M. (2019, December). A proposed secure mobile money transfer system for SME in Bangladesh: An industry 4.0 perspective. In 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-6). IEEE.
21. Junior, A. P., Díez, L. E., Bahillo, A., & Eyobu, O. S. (2023). Remote Pedestrian Localization Systems for Resource-Constrained Environments: A Systematic Review. IEEE Access.
22. Kafeero, S. (2022, July 21). Uganda's banks have been plunged into chaos by a mobile money fraud hack. Quartz. https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters
23. Kemp, S. (2023, February 14). Digital 2023: Uganda — DataReportal – Global Digital Insights. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-uganda#:~:text=Data%20from%20GSMA%20Intelligence%20shows,total%20population%20in%20January%202023.
24. Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1991). Authentication in distributed systems: Theory and practice. ACM SIGOPS Operating Systems Review, 25(5), 165-182.
25. Mega, B. (2020). Framework for improved security on usage of mobile money application based on iris biometric authentication method in Tanzania (Master's Dissertation). The University of Dodoma, Dodoma. http://hdl.handle.net/20.500.12661/2675 Downloaded from UDOM Institutional Repository at The University of Dodoma, an open access institutional repository.
26. Mirembe, D. P. (2015). The threat nets approach to information system security risk analysis. Rijksuniversiteit Groningen.
27. Mirembe, D.P, Lubega, T.J and Kibukamusoke, M. (2019). Leveraging Social Media in Higher Education: A Case of Universities in Uganda. European Journal of Open, Distance and E-learning.
28. Monitor., (2021, January 2). Mobile money shutdown hits businesses hard. Monitor. https://www.monitor.co.ug/uganda/business/finance/mobile-money-shutdown-hits-businesses-hard-1641168
29. Mousal, F. G. (2015, September 22). MTN denies UGX 21 billion mobile money dupery allegations. Techjaja. https://techjaja.com/mtn-denies-ugx-21-billion-mobile-money-dupery-allegations/
30. Mtaho, A. B. (2015). Improving mobile money security with two-factor authentication. International Journal of Computer Applications, 109(7).
31. MTN staff, cleaner and mobile money agent get 9 years for fraud. (2021b, January 19). Monitor. https://www.monitor.co.ug/uganda/news/national/mtn-staff-cleaner-and-mobile-money-agent-get-9-years-for-fraud-1611226
32. Namatovu, H. K. (2018). Enhancing antenatal care decisions among expectant mothers in Uganda (No. 164). PhD Thesis, University of Groningen, Netherlands. Available: https://www. rug. nl/research/portal/files/56325553/Complete_thesis. pdf Total Number/Percent of Mothers.
33. Nixon Kanali (2021). Africa's mobile fraud losses set to peak in 2021. From https://africabusinesscommunities.com/tech/tech-news/africa%E2%80%99s-mobile-fraud-losses-set-to-peak-in-2021/ on 16 May 2021 at 8:11am

34. Nzayinambaho, E. (2021). A Multifactor Authentication Security Model for Mobile Banking Transactions: The Case of A Mobile Banking System.
35. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.
36. Otiato Guguyu (2021). Survey finds half of mobile users lose cash to fraudsters. From https://www.businessdailyafrica.com/bd/economy/survey-finds-half-mobile-users-lose-cash-fraudsters-3654490#:~:text=The%20FinAccess%20survey%20found%20that,withdrew%20and%20refused%20to%20refund. On 16 May 2022 at 8:53 am
37. Parker, M. (2023, August 2). How can Africa guard against cybercrime? African Business. https://african.business/2023/08/african-banker/how-can-africa-guard-against-cybercrime
38. Paula Gilbert, (2021). Kenya, SA worst hit by mobile payment fraud. From https://www.connectingafrica.com/author.asp?section_id=761&doc_id=769857#:~:text=%22In%20the%20Middle%20Eastern%20and,%2C%22%20Lotfi%20told%20Connecting%20Africa. On 16 May 2022 at 7:44am
39. Pukkasenung, P., & Chokngamwong, R. (2016). Review and comparison of mobile payment protocol. In Advances in parallel and distributed computing and ubiquitous services (pp. 11-20). Springer, Singapore.
40. Ranyali, N. (2019). Conceptual Framework for Multi-Factor Authentication for Mobile Money Systems in Lesotho (Doctoral dissertation, Botho University).
41. Sanni, M. L., Akinyemi, B. O., Akinwuyi, D., Olajubu, E. A., & Aderounmu, G. A. (2023). A Predictive Cyber Threat Model for Mobile Money Services. Annals of Emerging Technologies in Computing (AETiC), 7(1), 40-60.
42. Sara Jerving (02 February 2023). Two types of drugs kill nearly 500,000 in sub-Saharan Africa each year. From https://www.devex.com/news/two-types-of-drugs-kill-nearly-500-000-in-sub-saharan-africa-each-year-104895#:~:text=Global%20Health-,Two%20types%20of%20drugs%20kill%20nearly,sub%2DSaharan%20Africa%20each%20year&text=Nearly%20half%20a%20million%20people,Office%20on%20Drugs%20and%20Crime. On 23 October 2023 at 9:02 PM
43. Serugo, G. (2023, April 12). BOU to banks: stop hiding cash thefts. The Observer - Uganda. https://www.observer.ug/news/headlines/77444-bou-to-banks-stop-hiding-cash-thefts
44. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188.
45. Telecoms, bank hacked, over sh1b stolen. (n.d.-b). New Vision. https://www.newvision.co.ug/news/1528751/telecoms-bank-hacked-sh1b-stolen
46. Tumwebaze, R. P. (2016). Decision Enhancement for Poultry Farmers in East Africa. Rijksuniversiteit Groningen.
47. Understanding cybercrime in Uganda. (2024, April 5). Monitor. https://www.monitor.co.ug/uganda/brand-book/understanding-cybercrime-in-uganda-4548288
48. UNODC report. (2023, February 1). Fake medicines kill almost 500,000 sub-Saharan Africans a year: UN News. https://news.un.org/en/story/2023/02/1133062
49. Zhaomiao Xu,Tao Zhang,Yujun Zeng, Jia Wan, Wuyang Wu (2015). A Secure Mobile Payment Framework Based On Face Authentication. Proceedings of the International MultiConference of Engineers and Computer Scientists 2015 Vol I, IMECS 2015, March 18 - 20, 2015, Hong Kong.
50. Zhou, Y., Wu, N., Hu, B., Zhang, Y., Qiu, J., & Cai, W. (2022). Implementation and Performance of Face Recognition Payment System Securely Encrypted by SM4 Algorithm. Information, 13(7), 316.