future internet

MDPI

Review

Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures

Guma Ali [1,*], Mussa Ally Dida [1] and Anael Elikana Sam [2]

[1] Department of Information Technology Development and Management (ITDM), Nelson Mandela African Institution of Science and Technology (NM-AIST), Arusha 447, Tanzania; mussa.ally@nm-aist.ac.tz

[2] Department of Communication Science and Engineering (CoSE), Nelson Mandela African Institution of Science and Technology (NM-AIST), Arusha 447, Tanzania; anael.sam@nm-aist.ac.tz

* Correspondence: gumaa@nm-aist.ac.tz; Tel.: +256-779-59-7131

Received: 9 August 2020; Accepted: 18 September 2020; Published: 24 September 2020

Abstract: The proliferation of digital financial innovations like mobile money has led to the rise in mobile subscriptions and transactions. It has also increased the security challenges associated with the current two-factor authentication (2FA) scheme for mobile money due to the high demand. This review paper aims to determine the threat models in the 2FA scheme for mobile money. It also intends to identify the countermeasures to overcome the threat models. A comprehensive literature search was conducted from the Google Scholar and other leading scientific databases such as IEEE Xplore, MDPI, Emerald Insight, Hindawi, ACM, Elsevier, Springer, and Specific and International Journals, where 97 papers were reviewed that focused on the topic. Descriptive research papers and studies related to the theme were selected. Three reviewers extracted information independently on authentication, mobile money system architecture, mobile money access, the authentication scheme for mobile money, various attacks on the mobile money system (MMS), threat models in the 2FA scheme for mobile money, and countermeasures. Through literature analysis, it was found that the threat models in the 2FA scheme for mobile money were categorised into five, namely, attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against availability. The countermeasures include use of cryptographic functions (e.g., asymmetric encryption function, symmetric encryption function, and hash function) and personal identification (e.g., number-based and biometric-based countermeasures). This review study reveals that the current 2FA scheme for mobile money has security gaps that need to be addressed since it only uses a personal identification number (PIN) and a subscriber identity module (SIM) to authenticate users, which are susceptible to attacks. This work, therefore, will help mobile money service providers (MMSPs), decision-makers, and governments that wish to improve their current 2FA scheme for mobile money.

Keywords: two-factor; authentication scheme; authentication; mobile money; the mobile money system; mobile banking; threat models; countermeasures

1. Introduction

The exponential demand for mobile money services is radically transforming the lives of the large unbanked population in sub-Saharan Africa. The mobile money system (MMS) makes it possible to render diversified services at affordable costs to remote areas and low-income people. Therefore, Suri [1] defined a mobile money system as a payment account that sits on the user's mobile phone and is used to engage in financial transactions by going through a menu. In sub-Saharan Africa, MMS has spread at a remarkable speed and extends many benefits such as convenience, reliability, speed,

flexibility, and affordability [2]. Furthermore, it settles domestic financial matters, avoids security hazards of carrying hard cash, and eliminates standing in long queues at banks [3].

In Uganda, mobile money payment systems such as MTN Uganda, Airtel, UTL, Africell, M-Cash, Ezeey Money, and Micropay have a combined network of approximately 200,857 agents who act as intermediaries [4–6]. These MMSs provide services ranging from sending and receiving the money to checking account balances [7,8]. Mobile money agents and users interact with the MMS using the unstructured supplementary service data (USSD) protocol interface that has a main menu and short message service (SMS) sent by the telecommunication company for notification purposes.

Although MMS plays an essential part in bridging the financial inclusion gap, unfortunately, the security of MMS has been a rising concern with the evolution of mobile technology. Despite the considerable effort invested in providing a more robust and secure system, most of the existing MMSs still rely on a weak two-factor authentication (2FA) scheme. Various attacks to mobile money's 2FA scheme include man-in-the-middle (MITM) attack, authentication attack, replay attack, identity theft, USSD technology vulnerabilities, brute force attack, social engineering attacks, and denial of service (DoS) attack [8–22]. Reaves et al. [23] also observed that the current MMS uses nonstandard cryptography, which is easily compromised, thus limiting the integrity and privacy guarantees of the software, giving rise to the threat of forged transactions and loss of transaction privacy.

In Uganda, many customers and businesses have lost billions of shillings to adversaries because of the sophisticated technologies used to attack MMS's 2FA, which is the weakest authentication method [24]. The purpose of this study is to analyse critically the previously published literature on the threat models and countermeasures for the mobile money's 2FA scheme. The MMS primarily deals with high-level private financial and confidential information, where the security has to be top-notch as threats cannot be accepted [7]. Therefore, deploying highly secure MMS will ensure secure authentication, access control, integrity, confidentiality, availability, nonrepudiation, and privacy of the confidential information [25,26].

There are related survey papers that focused on mobile 2FA schemes. For example, Ferrag et al. [27] presented a comprehensive review of smart mobile device authentication schemes. Phipps et al. [20] explored the security of the phone-based mobile money systems against attacks via the SIM interface. Han et al. [28] and Dmitrienko et al. [29] analysed the security of the 2FA schemes for the mobile. Nevertheless, none of the mentioned surveys analysed the threat models and countermeasures for mobile money's 2FA scheme. Therefore, this is the first study that thoroughly analyses the threat models and countermeasures of the 2FA scheme for mobile money in Uganda.

The current review makes the following contributions:

- Presents the concept of authentication and types of authentication factors.
- Presents an overview of the MMS architecture and mobile money access.
- Explains the authentication scheme for mobile money in Uganda.
- Discusses the five categories of the threat models, namely, attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against availability.
- Provide countermeasures for the threat models in mobile money's 2FA scheme.

The organisation of the paper is as follows: Section 2 presents related works on MMS architecture, mobile money access, the authentication scheme for the mobile money in Uganda, various attacks on MMS, threat models, and countermeasures; Section 3 presents the materials and methods used in the study; Section 4 details results and discussions; the final remarks and future works are given in Section 5.

2. Related Work

2.1. Concept of Authentication

Authentication is defined as the process of verifying the user's claimed identity by comparing the data received from an individual with those stored in the database to attest whether the person is who they claim to be [30]. Authentication is important because it allows only authorised individuals to access system resources [31]. The main mechanisms that are available to authenticate individuals with established credentials are as follows:

- Something you know (knowledge factor) such as a password, personal identification number (PIN), an answer to a security question.
- Something you have (ownership factor) such as security token, subscriber identity module (SIM) card, one-time password (OTP) token, employee access card.
- Something you are (biometric factor) such as biometric fingerprint, face, iris, retina, voice, gait, keystroke dynamics, gaze gestures, signature, deoxyribonucleic acid (DNA).

2.2. Types of Authentication Factors

There are mainly three types of authentication factors available to verify both online and offline users.

- Single-Factor Authentication (SFA) Single-factor authentication was defined by Rouse [32] and Rahav [33] as the process via which a person seeking access requests an authenticating party to attest their personality by availing a single attribute linked to the identity, for example, the use of a PIN to unlock a phone. Many companies accepted SFA because it is simple and user-friendly [34]. However, this form of authentication cannot be applied to financial institutions and other relevant transactions because it is vulnerable to shoulder surfing attacks, brute force attacks, social engineering attacks, and impersonation attacks [33].
- Two-Factor Authentication (2FA) Two-factor authentication was defined by Rahav [33] as the process via which a person seeking access requests an authenticating party to attest their personality by availing two attributes such as something you know and either something you have or something you are that are linked to the identity. Mobile money authentication, for example, relies on 2FA. In 2FA, the attacker must have the two identifiers for access [33]. Nevertheless, the 2FA is susceptible to eavesdropping, MITM attack, and forgery or Trojan horse attack and is not fully effective against phishing [34].
- Multifactor Authentication (MFA) Rahav [33] defined MFA as the process via which a person seeking access requests an authenticating party to attest their personality by availing multiple identifiers such as something you know, something you have, and something you are that are linked to the identity to grant access. In MFA, three factors such as knowledge, ownership, and biometric are all used together during authentication [33]. Many computing devices and critical services are adopting MFA because it provides higher levels of security against the different attacks [34,35]. MFA becomes more successful when one of the authentication factors is separated physically from the device from which the client accesses the application or resource [36]. The use of biometrics in the MFA process helps to improve identity proof and has a profound effect on the security of the system [34,37].

2.3. Mobile Money System Architecture

The MMS comprises several components such as network, customers, agents, administrators, authentication, financial institutions (e.g., banks), information technology (IT) administrators, base transceiver station (BTS), databases, and servers (telecom gateway servers such as short messaging service gateway (SMSGW) and USSD), core servers, web servers) [38]. The platform does not exist as a standalone unit; it connects to other mobile network operator (MNO) core elements to

access the global system for mobile communications (GSM) technology and to external platforms to provide full commercial functionality. The internal MNO interfaces include SMS centre (SMSC), USSD gateway, airtime in or mediation platform, web services, and interactive voice response (IVR) gateway. The external interfaces include banking systems, payment switches, biller systems, payment service provider systems, point-of-sale devices, and systems [39,40]. All these components work together to achieve the goal of the system. Figure 1 shows a mobile money system architecture.

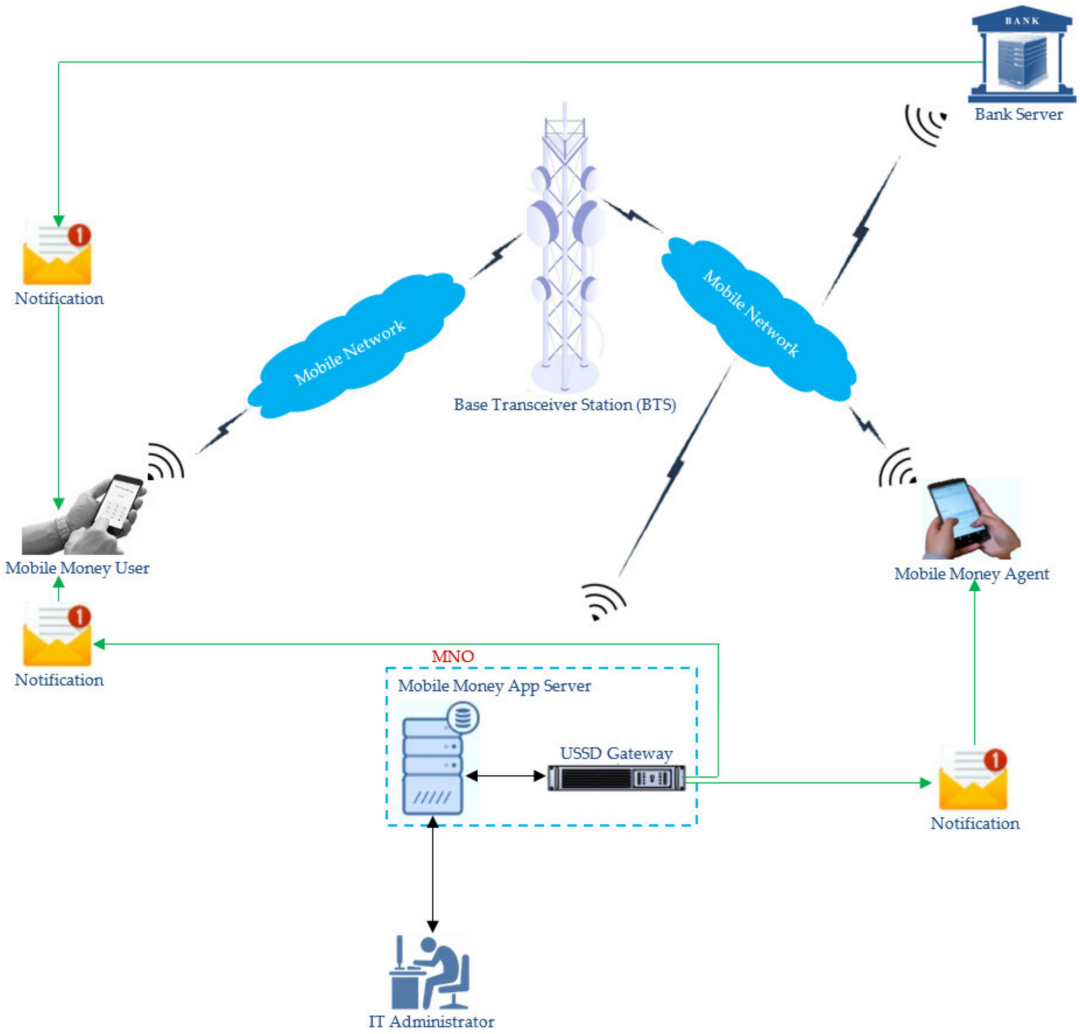

Figure 1. Mobile money system (MMS) architecture.

2.4. Mobile Money Access

In Uganda, mobile money applications have a standardised interface across the seven MMSPs. Varieties of acceptance technologies are available to mobile money merchants to access services from the servers, which include the following:

- Unstructured Supplementary Services Data (USSD): This is a communications protocol used by mobile communication technology in mobile networks to send texts between mobile phones and an application program without internet access [21]. It is session-based and interactive, but much faster since it involves simple operations that are handset-independent [39]. All seven MMSPs in Uganda, namely, MTN Uganda, Airtel, UTL, Africell, M-Cash, Ezeey Money, and Micropay, work by initiating a session between the mobile phone and the server through dialling a USSD code, for example, by dialling *165# in MTN to display the mobile money menu, followed by a

series of steps to accomplish a transaction [2]. There are two modes of USSD operations, namely, the mobile-initiated operation and the network-initiated operation [39].

- SIM Toolkit (STK): This is the portion of the GSM standard that enables the SIM to initiate activities to further exploit SMS by providing value-added services such as mobile banking [41]. GSMA [42] added that the STK is a set of applications that run on the SIM card and interact with the mobile device. Mobile operators use STK to present information about their services to subscribers [41]. The mobile money transaction is achieved when the mobile money platform breaks down the transaction into a series of logical steps by using STK and then reassembles the different steps into a complex statement, which is transmitted to the server via SMS [2].
- SMS: This is a technology used by mobile subscribers and mobile telephones to exchange alphanumeric messages [43]. All the mobile money platforms in Uganda use SMS to send confirmation or notification messages for the success or failure of a transaction to the user [2,39].

Mobile money platforms in Uganda have a simple interface made of a basic menu that is accessed using the USSD protocol. Mobile money users can send electronic money from their accounts to other users by interacting with the USSD interface and telecommunication company [2]. The telecommunication company sends a confirmation message to both the sender and the recipient about the money. The mobile money confirmation SMS contains details about the transaction identifier (ID), date and time of the transaction, amount sent, the recipient's name and phone number, the fee charged for sending the money, the reason for sending the money, and the available balance in the sender's account.

2.5. The Authentication Scheme for Mobile Money in Uganda

The current authentication scheme for mobile money uses a 2FA scheme where a subscriber must have a registered SIM card and mobile money PIN to perform a transaction. The SIM card has a unique phone number that is used as the account number for mobile money. The scheme has two main phases, namely, the enrolment phase and the authentication phase.

1. The Enrolment Phase

   The enrolment phase involves obtaining subscriber's details, including biodata, fingerprint, passport photo, national identification number (NIN) of the national ID, or valid passport and provisionally saving the information in the MNO's mobile money database. The NIN or passport number is verified from the national identification and registration authority's (NIRA) database. If the NIN matches with the one in the NIRA database, the subscriber is allowed to set the mobile money PIN. The subscriber's information is updated and saved in the database, and a confirmation message is sent to the subscriber for successful mobile money registration. If the NIN or passport number provided by the subscriber does not exist in the NIRA database, they are allowed to retry three times. If all the three attempts fail, a confirmation message is sent to the subscriber to try again. Figure 2 shows the data flow diagram for the mobile money enrolment phase.

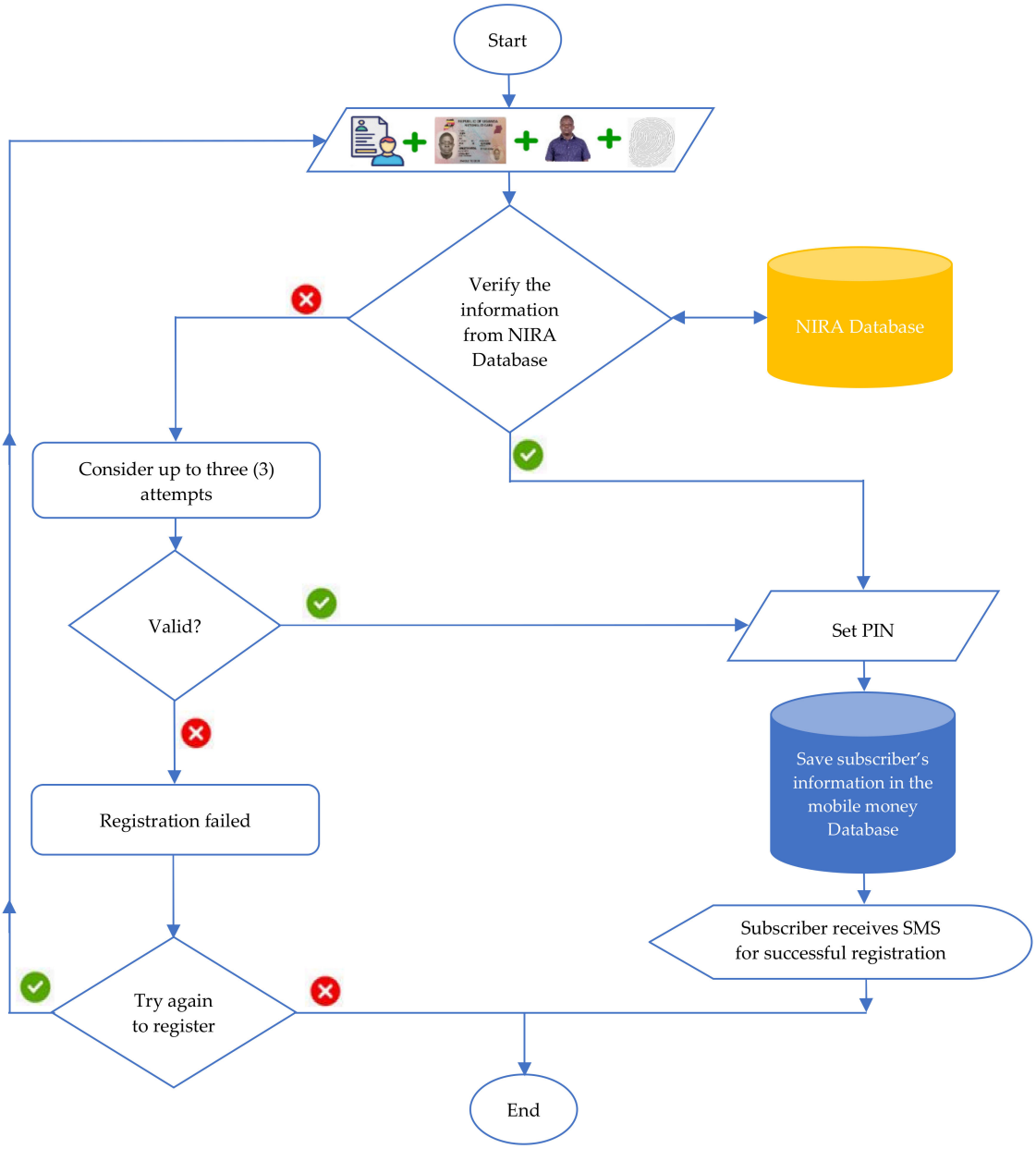

Figure 2. Mobile money enrolment phase.

2. The Authentication Phase

During the authentication phase, to send money to an MTN Uganda mobile user, the sender sticks to the following steps: (1) dial *165#, (2) select send money from the menu, (3) choose to send money to a mobile user, (4) enter recipient's phone number, and (5) enter amount. The amount entered is compared with the available electronic balance in the sender's account. If the amount is less than the amount entered, it terminates the transaction; otherwise, the sender continues. Then, (6) enter the reason for sending, and (7) confirm by entering the PIN Code. The application server then authenticates the PIN. If the PIN is correct, the money is sent, and (8) the sender receives a confirmation message; otherwise, they are allowed to retry for the maximum of three times. Note that the confirmation message contains details about the amount sent, the recipient's name and phone number, the fee charged for sending the money, the reason for sending the money, the available balance in the sender's account, and the transaction ID. Figure 3 shows the data flow diagram for a mobile money authentication phase.

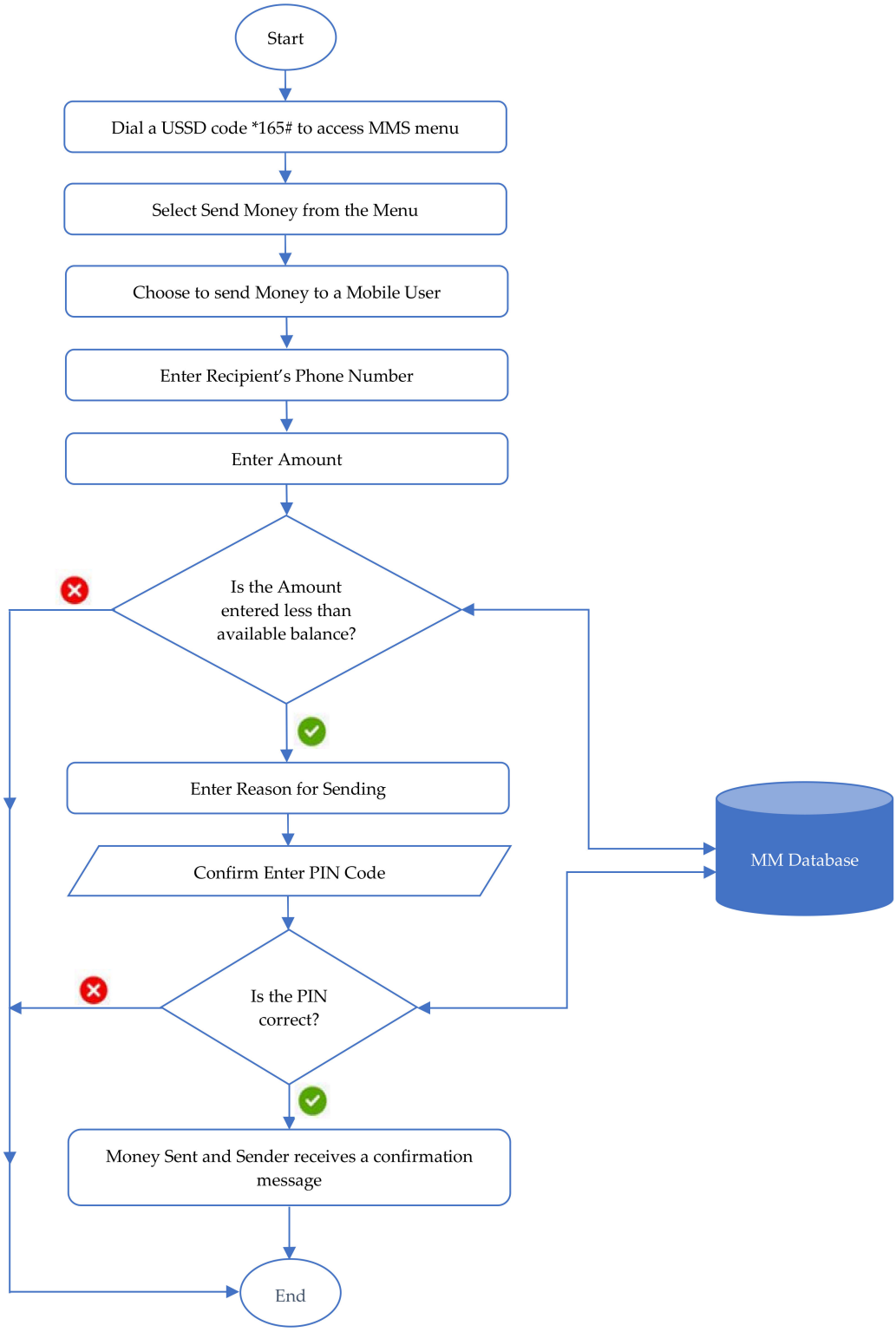

Figure 3. Mobile money authentication phase.

2.6. *Various Attacks on Mobile Money System*

An outsider or unauthorised person can attack the MMS at various levels. There are 11 attack points (AP) that are utilised by adversaries, as shown in Figure 4.

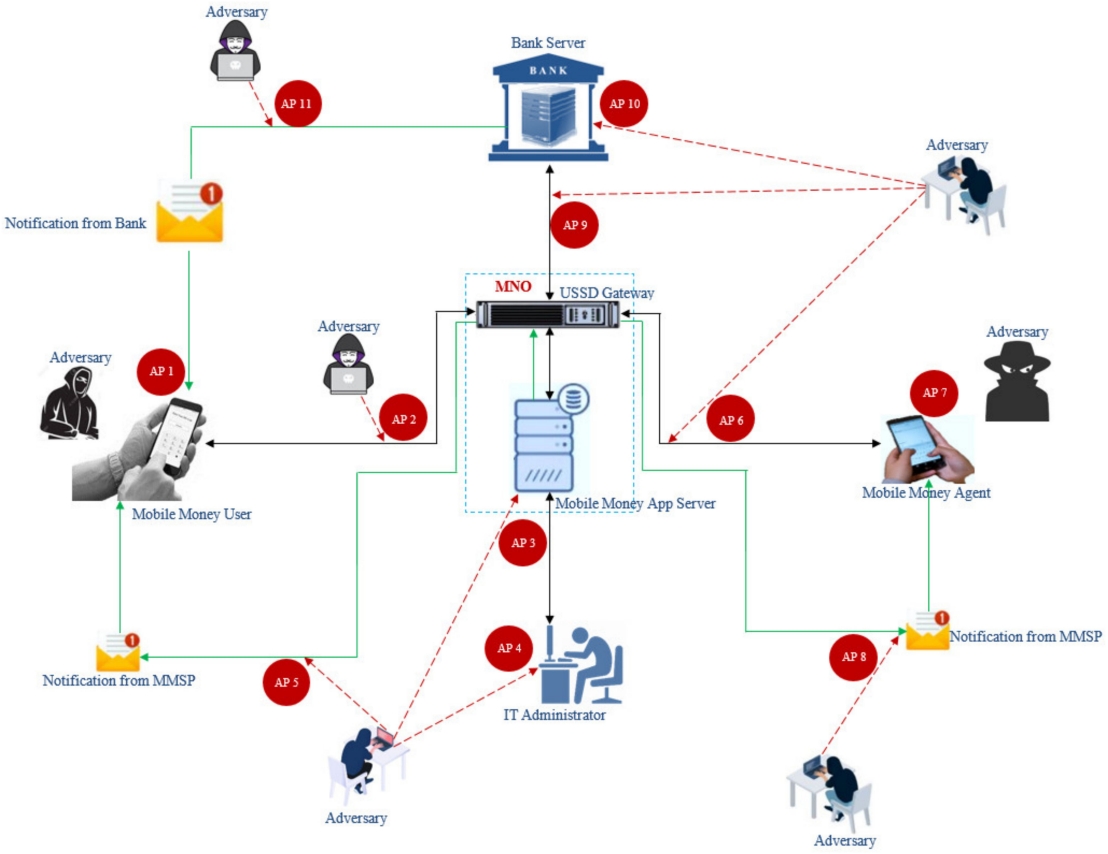

Figure 4. The red dashed line with an arrow represents an attack point (AP) on different components of the MMS.

- The attack on mobile money users, i.e., authentication attack at AP 1: The attacker gets access to the user's PIN through shoulder surfing since the PIN used is only four or five digits long and is unmasked [39]. Once the attacker accesses the PIN, they can perform a fraudulent transaction. The attacker can also perform a brute force attack because of the simplicity of the PIN [11,23,44].
- The attacks on the mobile money communication channels (AP 2, AP 6, AP 9): Attackers can hack or control the traffic into the MMS and manipulate accounts to perform transactions or gain benefits [11,23,44].
- The attack on the mobile money app server at AP 3: The adversary attacks the server and makes it unavailable to both mobile money users and agents. According to Castle et al. [11], attackers target mobile money servers and overwhelm them with fake traffic to block requests from mobile money users and agents. Attackers also install malware on the mobile money app server to deduct a small amount of money from the mobile money user's and agent's wallet and deposits it into the attacker's account without them realising [18].
- The attack on IT administrator (AP 4): The intruder, insider, or unauthorised person can hack into the administrator's computer and change the credentials so that the administrator cannot access the system.
- The attack on the mobile money agent (AP 7): The adversary uses a shoulder surfing technique to steal the agent's commission PIN or gives the wrong PIN repeatedly when making a transaction to get access to the agents' PIN. According to Buku and Mazer [12] and Lonie [13], the adversary gives the wrong mobile phone number repeatedly to get an agent's PIN and uses the PIN to gain unauthorised access to the agent's float account.

- The attack on the bank server (AP 10): The attacker makes the bank server unavailable to the mobile money user who wishes to transfer money from the bank account to the mobile money wallet through a denial-of-service attack.
- The attacks on notification message channel and modifications of messages (AP 5, AP 8, AP 11): Attackers can hack into the communication channel of the notification message, modify the message, and later resend it to the intended recipient [45,46].

2.7. Threat Models

MMS is a target for adversaries, authorised users, disgruntled employees, and system administrators possessing knowledge of the MMS. They gain access to the MMS to access the financial records of mobile money users and agents. The attacks on MMS can be internal or external and passive or active. Therefore, the current 2FA scheme protects and secures the MMS from security vulnerabilities and attacks. A threat model describes the attacks, the purpose of the attacks, the venues of attack that adversaries will exploit in their attempts to circumvent a system, and the mitigation measures prioritised. The threat models for mobile money's 2FA scheme are classified into five main categories, namely, attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against availability.

2.7.1. Attacks against Privacy

According to Makulilo [47], privacy is a person's right to be free from infringement or intrusion by others. Privacy attacks in mobile money are based on compromising the PIN of the subscribers so that the attacker can use it to illegally access the financial details of the victim and perform illicit transactions. An attacker or hacker can steal a user's information and identity, and this can cause serious problems not only to the victim but also to the overall economy [48]. MMS has databases that contain financial records of the users; attackers can illegally gain access to the mobile money database to steal the PINs of mobile money users and agents, and update or delete the records from the system. Furthermore, mobile money SIM card registration by MNOs taps a bunch of personal information about mobile users and agents such as names, NIN, mobile telephone numbers, e-mail addresses, and so on, thus generating databanks where MNOs have control and access to this personal information without appropriate privacy safeguards [47]. The availability of such transaction data opens the door for abuse by unscrupulous insiders and government officials. Mobile money user's privacy is also exposed during withdrawal and depositing of money where mobile money agents record their financial details in a book given by the MNOs. Nevertheless, these details are left with the mobile money agents for other purposes, thus posing privacy concerns [47]. Furthermore, illiterate users normally request the assistance of the agents to perform transactions on their behalf where their mobile money PINs are shared with the agents [49]. Therefore, this private information about mobile money users and agents must be protected from unauthorised access.

2.7.2. Attacks against Authentication

This category is where attackers forge identities to impersonate authorised mobile money users to gain access to the system. Ali, Dida, and Sam [8] further defined an authentication attack as a crime where attackers target and exploit the mobile money authentication process by applying a brute force attack against the PIN. Mobile money authentication attacks are classified into seven, namely, impersonation attack, replay attacks, masquerade attack, spoofing attacks, social engineering attack, phishing attack, and Trojan horse attacks.

- ✘ Impersonation attacks: This is an attack where the adversary successfully assumes the identity of a legitimate mobile money user or agent to access either the MMS or the information and services of a registered user. People share their PINs among friends and families to perform transactions

on their behalf. In case an attacker gets access to such a PIN, they can use it to log in to their mobile money accounts, perform fraudulent transactions, or change their PIN [8,9,12,13,46,50–52].

- ✘ Replay attack: This is where an attacker eavesdrops on network communication between the mobile money user and MMS, intercepts the data packets that include the PIN, and then fraudulently delays or resends it to the recipient. This takes place in the form of eavesdropping on mobile communication, and mobile money platforms use SMS to notify mobile money users and agents. The SMS is protected using weak algorithms like the A5 and attackers with scanning software can easily intercept, modify, and resend them [45,46,50,53]. The attacker can misuse the previously exchanged messages between the mobile money user and MMSP to perform the replay attacks [43].
- ✘ Masquerade attack: A masquerade attack is an attack where an adversary obtains the subscribers' SIM card and PIN and uses them either to request money from legitimate user's friends and relatives or to perform fraudulent transactions. This occurs when the attacker obtains the credentials of the authorised user through social engineering techniques and uses them to swap the SIM card. Furthermore, the adversary can also use fake documents to register the SIM cards of legitimate users and have full access to the mobile money account of the victims [14,45,50,51].
- ✘ Spoofing attacks: This attack occurs when the adversary assumes the role of a mobile system administrator and has full access to the system. This is common because most mobile money applications and systems are poorly protected, thus giving opportunity for the attackers to hack them [16,23].
- ✘ Social engineering attack: This is the manipulation of people to reveal confidential information like mobile money PIN so that the attacker can gain control over the user's mobile money account [19]. Mobile money platforms use PINs for securing mobile money accounts, which makes them vulnerable to many security threats, including social engineering attacks [19]. Attackers use social engineering techniques to circumvent mobile money's 2FA scheme, compromise user accounts, and avoid fraud detection technologies [19].
- ✘ Phishing attacks: This is a deceitful attempt by adversaries to obtain confidential information such as mobile money PINs from mobile money users and agents by impersonating employees of MMSP in electronic communication. Ali, Dida, and Sam [8] further expanded the definition as "a form of mobile money crime where fraudsters masquerade as employees of the MMSP by calling or sending SMS messages to mobile money users and agents to reveal their data including PINs for an update" (p. 18). Phishing starts when an adversary intercepts the network traffic between the mobile money user or agent and the mobile money application server and then uses a fraudulent call or message to lure the victim into revealing their credentials. The message is created to look as if it comes from the MMSP. Then, the victim is persuaded into providing the mobile money PIN to the fraudster [11].
- ✘ Trojan horse attacks: A Trojan horse is malicious software that, once installed on a phone, either steals sensitive information and sends it to the attacker or creates a backdoor for the attacker to have access to the phone. It uses a Trojan horse program employed by hackers and adversaries to compromise the authentication system. Mobile money users and agents are tricked by some form of social engineering into loading and executing Trojans on their phones. Once activated, Trojans can enable hackers to spy on mobile money users and agents, steal their mobile money PINs, and gain backdoor access to their mobile money accounts [19,26,48]. Moreover, adversaries can install malware that gives them the exclusive right to redirect users to their network [14].

2.7.3. Attacks against Confidentiality

This category is where an attacker eavesdrops on the communication channel between the mobile money user and the mobile money application server or bank to tap information like the mobile money PIN that is used to compromise the system. Confidentiality attacks in mobile money are classified into four, namely, eavesdropping attacks, brute force attacks, guessing attacks, and shoulder surfing attacks.

- Eavesdropping attacks: This is where an attacker secretly overhears information transmitted over the communication channel between the mobile money application server and mobile money user, the mobile money application server and mobile money agent, or the bank server and mobile money application server, without being authorised by the trusted parties. The attacker takes advantage of unsecured network communications to access sensitive information. This is common when the data transmitted over the communication channel are in plaintext [21,54]. Mtaho [52] observed that attackers use network sniffer software such as Wireshark to intercept data in transit. Furthermore, attackers also take advantage of weak encryption keys used and the weak secure sockets layer (SSL)/transport layer security (TLS) implementation, which gives them the opportunity to snoop the communication channel [23].
- Brute force attacks: This is where an adversary guesses the PIN of a mobile money user or agent to gain access to their mobile money account. It is a simple attack method and has a high success rate because MMS uses numeric PINs to authenticate users [8,9,11,23,46,52,55]. Kunda and Chishimba [19] also observed that, in authenticating users using a smartphone, when the PIN is entered several times, it might leave a greasy residue or scratches on the touch screen, which may make it easy for the attacker to guess. Brinzel, Anita, and Shraddha [56] and Aloul, Zahidi, and El-Hajj [57] concluded that using a PIN for authentication is vulnerable to a brute force attack.
- Guessing Attack: This attack occurs when an adversary happens to see the mobile money PIN of the subscriber during the authentication process. The PIN used for authenticating the user has only four or five digits and is entered when unmasked, thus making it guessable [9,23,52,55].
- Shoulder Surfing attack: This is where an attacker obtains information such as PINs and other confidential data by looking over the victim's shoulder while performing a mobile money transaction. Attackers take advantage of crowded places where mobile money agents operate and where mobile money users perform transactions. The mobile money PIN used for authenticating a user is simple and unmasked, thus making it easy for the attacker to see and memorise [19,39,57,58].

2.7.4. Attacks against Integrity

This category is where an attacker accesses and modifies the user information in the MMS. Attacks against integrity are classified into three, namely, MITM attack, salami attack, and insider attacks.

- MITM attack: This is an attack where the intruder intercepts communications between mobile money users and the MMS, between mobile money agents and MMS, between mobile money users and the bank, or between the MMS and the bank and becomes familiar with the messaging system, thereby transmitting fake data to either party. The attacker sits between mobile money users and the MMSP and makes them believe that they are communicating directly to each other, when in fact the adversary controls the entire conversation [11,46]. According to Mahajan, Saran, and Rajagopalan [44] and Reaves et al. [23], the attacker controls the traffic into the mobile money platform to manipulate the credentials of the user and to perform transactions on behalf of the victim. Likewise, the adversary can use a BTS with the same mobile network code as the subscriber's real network to perform a MITM attack since the network authenticates users [26,43,45]. Furthermore, the information carried within the communication channel is in plaintext, thus making USSD data vulnerable to attack and redirection [20,21,52].
- Salami attack: This is where an employee of a financial institution installs a malware like a Trojan horse on the server hosting the application to withdraw a small amount of money from the subscribers' accounts and deposit it into their account. The salami attack can be internal or external and difficult to notice since the malware modifies the data in financial systems and a small amount is deducted from the customers' wallets [8,18,59–61].
- Insider attacks: This is where an employee of the MMSP who has enough information about the organisation's security practices, MMS, and data attacks the mobile money application server or MMS. According to Trulioo [62] and Musuva-Kigen et al. [10], insiders and employees of the

MMSP due to inside access facilitate most mobile money fraud. This has resulted in organisations losing huge amounts of money to the tune of billions of shillings because of employee fraud within the companies or institutions [10]. Additionally, Gilman and Joyce [49] and Trulioo [62] noted that less scrupulous employees abuse their privileges by accessing customer mobile money information and stealing money from customers' wallets.

2.7.5. Attacks against Availability

This category is where an adversary denies mobile money users and agents access to the mobile money application server or bank server, thus rendering the service unavailable. Attacks against availability include DoS and distributed DoS (DDoS) attacks and mobile phone theft.

- DoS and DDoS attacks: DoS attack is where attackers overwhelm mobile money server with fake traffic to block requests from legitimate users requesting to access the services. The DDoS attack, on the other hand, is a kind of attack where adversaries overwhelm the mobile money server from different sources, thus making it difficult to stop the attacks. The goal of DoS and DDoS attacks is to make mobile money services unavailable by flooding servers with an immense amount of data to make it busy and unable to provide services to legitimate users [11,45]. Additionally, when DoS and DDoS occur, mobile money agents, banks, and MMSPs lose money, and mobile money users cannot access their mobile wallet accounts [9,11,14,63].
- Mobile phone theft: According to Reaves et al. [23] and Castle et al. [11], when an attacker steals the mobile money user's or agent's mobile phone, the SIM card that has a wallet account becomes unavailable. It also results in loss of data and service access [64]. Moreover, an attacker can swap SIM cards for those of the mobile money users and agents and take over the victims' e-wallet account, thus making it unavailable for legitimate users [14,50,51,62].

Figure 5 summarises the classification of threat models in mobile money's 2FA scheme.

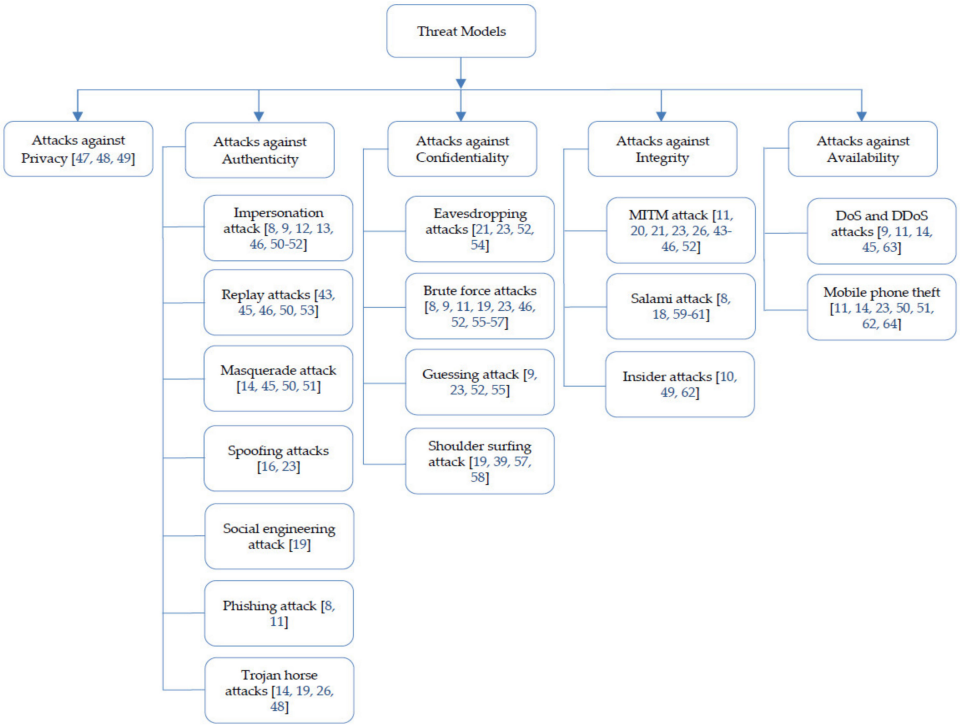

Figure 5. Classification of threat models in mobile money's two-factor authentication (2FA) scheme.

2.8. Countermeasures

For efficient and secure mobile money authentication, there is a need to prevent various attacks against the current 2FA scheme. Mobile money users, agents, and administrators can use both cryptosystem and non-cryptosystem measures to prevent the attacks to ensure secure mobile money authentication. The countermeasures are categorised into cryptographic functions and personal identification as shown in Figure 6.

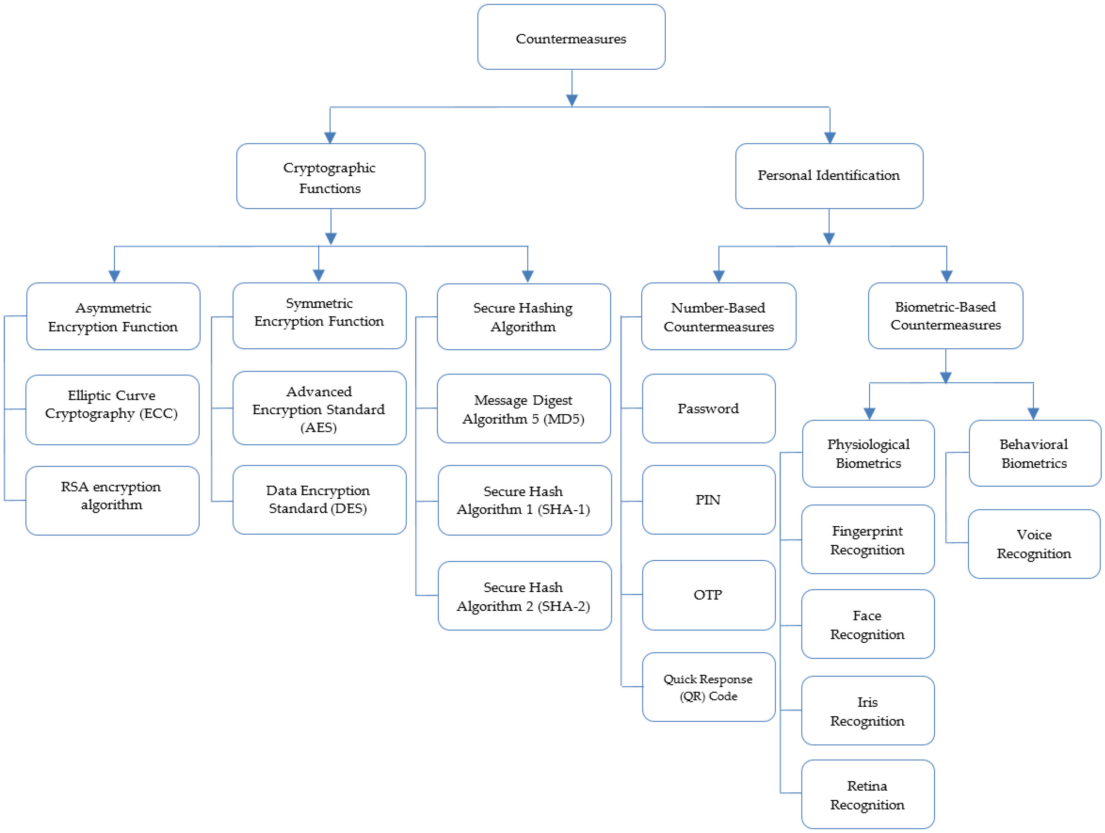

Figure 6. Countermeasures against attacks in mobile money's 2FA schemes.

2.8.1. Cryptographic Functions

Barker and Barker [65] defined cryptographic functions as cryptographic algorithms in conjunction with the modes of operation. In the 2FA scheme for mobile money, cryptographic functions help in achieving the security goals of confidentiality, authenticity, and integrity. The most common cryptographic functions used in the mobile money's 2FA scheme are asymmetric encryption function, symmetric encryption function, and hash function.

1. Asymmetric Encryption Function: The examples of asymmetric encryption functions used in the 2FA scheme for mobile money are elliptic curve cryptography (ECC) and the Rivest–Shamir–Adleman (RSA) encryption algorithm. The mobile money authentication schemes [66–70] use ECC. The scheme proposed by Bojjagani and Sastry [66] uses SMS, elliptic curve integrated encryption scheme (ECIES), and elliptic curve digital signature algorithm (ECDSA) to ensure user authentication, data confidentiality, and nonrepudiation, thereby reducing computation complexity in mobile banking. Using the elliptic curve Menezes-qua-Vanstone (EC-MQV) key agreement protocol in [67] gave resistance against MITM attacks, SIM cloning and swapping attacks, DoS attacks, and message modification. The scheme in [68] used biometric fingerprints or retinal images on the basis of ECC to provide strong security against MITM attacks, replay attacks, DoS attacks, spoofing attacks, and repudiation. Furthermore, the scheme is effective in terms of

computation and communication. Shilpa and Panchami [69] employed biometric, IMEI number, and SIM serial number, colour encryption with ECC to improve the security of mobile banking. The scheme [70] integrated secure ECC to provide data confidentiality, data integrity, and user authentication in mobile banking. The scheme proposed by Sharma and Bohra [71] employed a hybrid cryptographic authentication method using the quick response (QR) code and OTP to improve user authentication and confidentiality in online banking. Additionally, using the encrypted QR code with RSA in the scheme in [72] ensured the legitimacy of the user, information confidentiality, integrity, and accuracy in mobile payment.

2. Symmetric Encryption Function: The examples of symmetric encryption functions used in mobile money authentication include data encryption standard (DES) and advanced encryption standard (AES). Using triple-DES (3DES) in [73] provided more security in a cashless transaction than DES. The scheme proposed by [74] used a PIN, SIM card, and face recognition with a DES/3DES encryption algorithm to enforce the security between the mobile payment application and the virtual private ad hoc network. Alornyo et al. [75] employed identity-based cryptography in securing mobile money wallets to resist insider attacks, and it consumed less computational cost in token generation. The scheme proposed by [76] used a dynamic mobile phone token, SSL protocol, and AES to encrypt the transaction information and combat MITM attacks, replay attacks, and transactions repudiation. The scheme in [56] used a QR code with AES-128 bit encryption–decryption and secure hash algorithm 1 (SHA-1) for securing Android smartphones from attacks.
3. Secure Hash Function: The MD5, SHA-1, and SHA-2 are common examples of hash functions used in mobile money authentication. Alhothailya et al. [77] proposed an authentication scheme for online banking using a one-time-username and SHA-1 hash function to calculate the ticket's hash value. Using a vehicle's identity and the SIM to secure the mobile money authentication system in [78] offered higher security against the increasing identity thefts, SIM cloning, and other cybercrimes.

2.8.2. Personal Identification

The personal identification is further categorised into number-based countermeasures and biometric-based countermeasures.

1. Number-Based Countermeasures: The examples of number-based countermeasures used in mobile money authentication include password, PIN, OTP, and QR code.

    - Password: A password is a string of characters including letters, digits, or symbols that a user memorises secretly to confirm their identity. An authentication party verifies the identity of a person to access a service. It is a requirement that the password should be long (at least eight characters), a mixture of both uppercase and lowercase letters, as well as letters and numbers, and should include special characters. Similarly, a password must be changed frequently and easy to remember, but a nondictionary word so that it is hard for an attacker to guess. In most cases, the password is used alongside a username during authentication. Authentication schemes in [79–81] used a password to enhance the security of mobile money. The scheme in [80] integrated username and password, phone number, and voice biometric solutions during the authentication of M-Pesa transactions. The scheme in [81] employed username, password, and fingerprint in mobile banking transaction. The password remains the weakest component of many authentication systems [82].
    - PIN: Hao-Jun, Wei-Chi, and Yu-Xuan [83] defined a PIN as a numeric key used for authenticating users in an electronic transaction. For user convenience, PINs are often short (up to eight digits) to allow access to only authorised users. PINs are widely used for user authentication such as withdrawing cash from mobile money or withdrawing money from an automated teller machine (ATM) [84]. Mtaho [52], Islam [85], Ombiro [86],

Singh and Jasmine [87], Fan et al. [88], Islam et al. [89], and Zadeh and Barati [90] employed authentication schemes using PINs to verify user identity. Using PINs, the schemes in [86,87,90] provided convenience, efficiency, reliability, and security in mobile transactions. Moreover, the schemes in [52,85,89] used PINs to achieve better dependability and customer satisfaction. The PIN should be easy to remember, random, and hard to guess, while it should be changed frequently, distinct for different accounts, and not written down or stored in plaintext [52]. However, using a PIN in mobile money authentication is susceptible to shoulder surfing attacks, brute force attacks, and smudge attacks [83,84,91].

- OTP: Elganzoury, Abdelhafez, and Hegazy [92] defined OTP as a unique and time-sensitive string of alphanumeric characters generated and forwarded to the user's mobile phone via either email or SMS for a single authentication session. Clock time-based OTP, pattern-based OTP, and random key-based OTP are the three methods used to generate OTP on the basis of the secret key derived from the Diffie–Hellman algorithm [93,94]. The OTP generator located on the server machine creates the OTP and sends it to the user to complete the authentication process [95,96]. If an adversary succeeds in accessing the OTP, they may not be able to predict the next because of its random generation. The authentication schemes in [71,79,86,87,90,97,98] employed OTP, which is fast, efficient, reliable, and convenient. Furthermore, it is resistant to phishing attacks, identity theft, guessing attacks, brute force attacks, and unauthorised access by attackers.
- QR Code: A QR Code is a two-dimensional barcode encoded using standardised modes to store information that can be read using an imaging device such as a smartphone camera [99]. The swift expansion of QR code in mobile wallets is because of ease of use, security, cost-effectiveness, and trackability [100,101]. The schemes proposed by [56,71,100,102,103] employed QR codes to ensure convenience, accuracy, confidentiality, nonrepudiation, integrity, speed, and safety in payment transactions. Additionally, it offers resistance against impersonation attack, shoulder-surfing attack, identity theft, and brute force attack.

2. Biometric-Based Countermeasures: Biometrics are the unique physical or behavioural characteristics used to verify a person's identity [30]. There are two types of biometrics, namely, physiological biometrics and behavioural biometrics.

    - Physiological biometrics: Physiological biometrics use the physical characteristics of a person to determine their identity. Examples of physiological biometrics used in mobile money authentication include fingerprint recognition, face recognition, iris recognition, and retina recognition. Islam [85], Mtaho [52], Ahsan et al. [104], Fan et al. [88], Okpara and Bekaroo [105], Sharma and Mathuria [81] used fingerprint recognition in mobile money authentication to offer security against identity theft, shoulder surfing attack, replay attack, impersonation attack, and counterfeit, and it was responsible for privacy protection. The scheme in [90] used facial recognition in authentication to increase the security and reliability of mobile banking systems. Using iris recognition, the scheme in [89] helped to achieve better efficiency, accuracy, dependability, customer satisfaction, and security during mobile money authentication. Moreover, the scheme in [68] employed retina recognition in mobile money authentication to provide security against MITM attack, replay attack, DoS attack, spoofing attack, and repudiation.
    - Behavioural biometrics: Behavioural biometrics depend on an individual's behavioural characteristics to identify them. Voice recognition is the only example of behavioural biometrics used in mobile money authentication. The authentication schemes in [80,86] used voice recognition to increase efficiency, convenience, and security, as well as to resist impersonation attack.

Table 1 summarises the countermeasures against the attacks in mobile money authentication schemes.

Table 1. Summary of the countermeasures against the attacks in mobile money authentication schemes.

S/No	Countermeasure		Scheme
1	Asymmetric encryption function	ECC	[66–70]
		RSA encryption algorithm	[72]
2	Symmetric encryption function	DES	[73–75]
		AES	[56,76]
3	Secure hash function	SHA-1	[77,78]
4	Number-based countermeasures	Password	[79–81]
		PIN	[52,83–91]
		OTP	[71,79,86,87,90,97,98]
		QR Code	[56,71,100,102,103]
5	Biometric-based countermeasures	Fingerprint recognition	[52,81,85,88,104,105]
		Facial recognition	[90]
		Iris recognition	[89]
		Retina recognition	[68]
		Voice recognition	[80,86]

3. Materials and Methods

A comprehensive literature search on the threat models and countermeasures for the 2FA scheme in mobile money was conducted using digital library databases. Some of the databases used include IEEE Xplore, MDPI, Emerald Insight, Hindawi, ACM, Elsevier, Springer, Google Scholar, and Specific and International Journals. Specific keywords such as "2FA scheme for mobile money", "2FA protocol for mobile money", "2FA framework for mobile money", "2FA scheme for mobile wallet", "2FA protocol for mobile wallet", "2FA framework for mobile wallet", "2FA scheme for mobile banking", "2FA protocol for mobile banking", and "2FA framework for mobile banking" were used to identify the literature for the study. The researchers only reviewed papers related to the 2FA scheme, and each collected source was evaluated against relevance, originality, eminence, influence, and year of publication. Furthermore, the researchers omitted some papers whose content was outside 2FA schemes and not written in English. The selected collection of literature comprised the most relevant papers in the area of the 2FA scheme for mobile money as the primary objective. Ninety-seven papers were reviewed, of which 28 were from the IEEE Xplore, three from MDPI, two from Emerald Insight, three from Hindawi, six from ACM, three from the Elsevier, six from Springer, 16 from Google Scholar, and 30 from Specific and International Journals, as summarised in Figure 7. Out of the reviewed papers, 39 papers focused on the threat models in the 2FA scheme for mobile money, and 58 focused on the countermeasures against the attacks in mobile money's 2FA schemes. The literature search started in January 2020 and continued until the date of the submission of the paper.

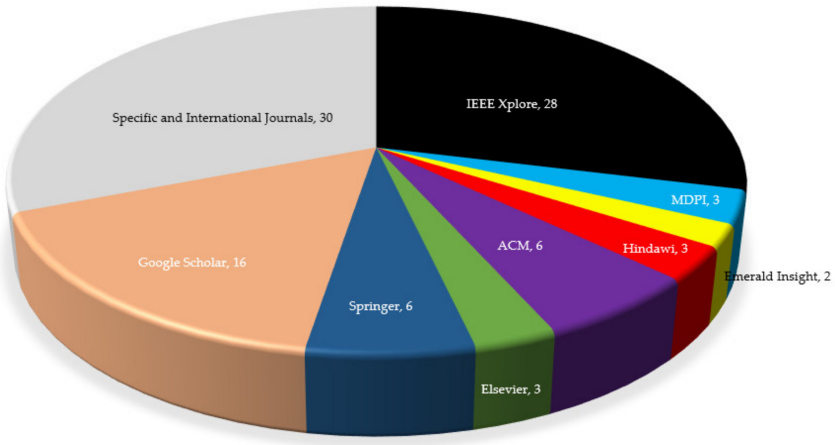

Figure 7. Summary of the number of research papers reviewed.

4. Results and Discussion

Through the literature analysis, the threat models below were identified and discussed.

- ✘ Attacks against privacy: In this attack, adversaries infringe on the privacy of mobile money users, agents, MNO, and the MMS. They also compromise the PINs of the subscribers so that the attacker can use them to illegally access the financial details of the victim and perform illicit transactions. Additionally, attackers take advantage of the illiteracy of mobile money users and agents to access their mobile money PINs and accounts. To deal with this attack, [71,106] proposed a hybrid cryptographic method on the basis of the MD5 algorithm and the RSA algorithm. Bojjagani and Sastry [66] and Salim, Sagheer, and Yaseen [70] suggested ECDSA for digital signature and ECIES using AES-GCM as the encryption algorithm. Makulilo [47] recommended general data privacy legislation and sector-specific laws that protect privacy. Moreover, digital communications law and user regulations in mobile money provide data privacy, confidentiality, and lawful interception.
- ✘ Impersonation attacks: An attacker can assume the identity of a legitimate mobile money user or agent, access the financial details of a registered user, and perform fraudulent transactions. There are 14 authentication protocols [56,66–70,72,77,81,87,88,102,103,105] to prevent impersonation attacks. The schemes in [81,105] employed fingerprint biometrics. Bojjagani and Sastry [66], Ray, Biswas, and Dasgupta [68], and Shilpa and Panchami [69] used elliptic curve cryptosystems. Singh and Jasmine [87], Kisore and Sagi [67], Rodrigues, Chaudhari, and More [56], Alhothailya et al. [77], and Salim, Sagheer, and Yaseen [70] adopted hashing functions. Purnomo, Gondokaryono, and Kim [72] proposed an asymmetric encryption function. The idea of mutual authentication was proposed in [72,88]. On the other hand, [102,103] used random values like OTP.
- ✘ Replay attack: An attacker eavesdrops on network communication between the mobile money user and MMS, and intercepts the data packets that include the PIN, and then delays and resends it to the recipient. To thwart this attack, [66,68,69,102,103] employed pairing-based cryptography and timestamps in encrypted data. Rodrigues, Chaudhari, and More [56] and Salim, Sagheer, and Yaseen [70] adopted techniques with hashing functions. Alhothailya et al. [77] proposed the use of a one-time username to secure the system against this attack.
- ✘ Masquerade attack: This is where an adversary uses social engineering techniques to obtain the subscribers' SIM card, PIN, or other credentials of the authorised users and uses them to request money from legitimate user's friends and relatives and to carry out illegal business. To resist masquerade attacks, [66,68,69] proposed deploying the elliptic curve cryptosystem. Purnomo, Gondokaryono, and Kim [72] and Fan et al. [88] adopted mutual authentication

techniques. Kisore and Sagi [67], Rodrigues, Chaudhari, and More [56], Sharma and Bohra [71], Alhothailya et al. [77], and Salim, Sagheer, and Yaseen [70] used the idea of hash functions. Coneland and Crespi [78], Okpara and Bekaroo [105], Sharma and Mathuria [81], Chetalam [80], and Islam et al. [89] proposed the use of physiological and behavioural biometrics.

- ✘ Spoofing attacks: An adversary can assume the role of a mobile system administrator and have full access to the system. The poor protection offered to most mobile money applications and systems allows the attackers to hack and control the systems. Security against this attack was ensured in [68,80,81,89,104,105,107] by using biometric authentication. Purnomo, Gondokaryono, and Kim [72] and Fan et al. [88] used mutual authentication techniques.
- ✘ Social engineering attack: Mobile money platforms use PINs to secure mobile money accounts, thus making them vulnerable to many security threats, including social engineering attacks. Attackers also use social engineering techniques to circumvent mobile money's 2FA scheme, compromise user accounts, and avoid fraud detection technologies. Security against social engineering attacks is ascertained using a multifactor authentication scheme, customer alert systems, and anti-phishing systems [108]. Luo et al. [109], Chinta, Alaparthi, and Koda [110], and Conteh and Schmick [111] adopted a multidimensional approach, including technology, policies, procedures, standards, employee training, and awareness programs. Hamandi et al. [112] proposed an anomaly-based intrusion detection system to thwart SMS messaging attacks.
- ✘ Phishing attacks: This is where fraudsters masquerade as staff of MMSP and call or send SMS messages to the subscribers to lure them into revealing their mobile money PIN. Resiliency against phishing attacks is enhanced by employing multifactor authentication, an anomaly-based intrusion detection system, email authentication, encryption, secure sockets layer, reports of suspicious activities, back-end analytics, user training and awareness, content-based filtering, blacklisting, and whitelisting [112–114]. Aleroud and Zhou [115] used machine learning, profile matching, text mining, ontology, honeypots, and client-server authentication to detect phishing attacks.
- ✘ Trojan horse attacks: Attackers use social engineering to trick mobile money users and agents into loading and executing Trojans on their phones. Once activated, Trojans can enable hackers to spy on mobile money users and agents, steal their mobile money PINs, and gain backdoor access to their mobile money accounts. The security against Trojan horse attacks was ensured in [68,69] by using the idea of integrating biometrics and cryptography. Jung et al. [116] proposed binary code obfuscation and hardware-based code attestation. Bosamia and Patel [106] adopted malware detection and prevention techniques.
- ✘ Eavesdropping attacks: This is where an attacker secretly overhears information transmitted over the communication channel without being authorised by the trusted parties. The attacker takes advantage of unsecured network communications to access sensitive information. Salim, Sagheer, and Yaseen [70] enforced security against eavesdropping attacks by using a message authentication code (MAC). Bojjagani and Sastry [66] proposed the use of ECIES and ECDSA.
- ✘ Brute force attacks: This is a simple attack method with a high success rate because MMS uses numeric PINs of four or five digits to authenticate users. To deal with brute force attacks, [56,70,77,87] proposed the use of cryptographic hash functions.
- ✘ Guessing attack: Mobile money users and agents use a PIN during mobile money authentication and the PIN used is only four or five digits, entered when unmasked, thus making it guessable. To thwart this attack, [66–70] employed the elliptic curve cryptosystem. Singh and Jasmine [87] adopted a password-salting mechanism. Rodrigues, Chaudhari, and More [56] and Alhothailya et al. [77] used hashing functions.
- ✘ Shoulder surfing attack: Attackers take advantage of crowded places to obtain mobile money agents' and users' PINs by looking over their shoulders while performing transactions. To resist this attack, [79–81,85,86,89,90,105] emphasised the use of sightless multifactor authentication.
- ✘ MITM attack: In this attack, the adversary sits between the mobile money user and MMSP and makes them believe that they are communicating directly with each other,

when in fact the attacker controls the entire conversation. There are different authentication protocols [56,66–71,73,74,76,79,85,86,90,102,103] that are resilient against MITM attacks. To deal with this attack, [66,69] proposed the use of ECC. Ray, Biswas, and Dasgupta [68] proposed the use of both biometric fingerprint and ECC, [79,85,86,90] used multi-factor authentication, and [56,67,70,71,73,74,76,102,103] proposed the use of symmetric encryption and message authentication code.

- ✘ Salami attack: This is where an employee of a financial institution installs a malware like a Trojan horse on the server hosting the mobile money application to withdraw a small amount of money from the subscribers' accounts and deposit it into their account. To thwart this attack, [18] suggested that there is a need to define an efficient and robust user and security policy that contains different privileges, updates security systems, initiates both SMS and email messages to alert customers regarding any transaction that occurs, and advises the customers to report any unaware money reductions.
- ✘ Insider attacks: This is where an employee of the MMSP who has enough information about the organisation's security practices, MMS, and data attacks the mobile money application server or MMS. To resist insider attacks, [66,68,70] used elliptic curve cryptography. Alornyo et al. [75] employed identity-based cryptography, and [117] proposed a certificate-based signcryption scheme.
- ✘ DoS and DDoS attacks: This is where attackers overwhelm mobile money servers with fake traffic to block requests from legitimate users requesting to access the services. The goal is to make mobile money services unavailable to legitimate users. Resiliency against DoS attacks is enhanced by using cryptographic hash functions [56,67,68,70,71,77,87]. Mtaho [52], Ahsan et al. [104], Okpara and Bekaroo [105], and Sharma and Mathuria [81] proposed the use of biometric fingerprint authentication. On the other hand, to deal with a DDoS attack, [118] introduced a nonlinear control approach that can prevent malicious attack packets. Cepheli, Büyükçorak, and Kurt [119] proposed a hybrid intrusion detection system that utilises anomaly- and signature-based detection methods.
- ✘ Mobile phone theft: When an attacker steals the mobile money user's or agent's mobile phone, the SIM card that has a wallet account becomes unavailable. Tu et al. [64] proposed technical countermeasures such as remote device wipe, training customers, access blocking, data encryption, online or offline data backup, remote access to built-in cameras, global positioning system (GPS) device tracking, and PIN protection.

Table 2 summarises the threat models and countermeasures.

Table 2. Summary of the threat models and countermeasures.

S/No	Threat Models	Countermeasure	References
1	Attacks against privacy	A hybrid cryptographic method using the MD5 algorithm and the RSA algorithm.	[71,106]
		ECDSA for digital signature and ECIES that uses AES-GCM as the encryption algorithm.	[66,70]
		General data privacy legislation and sector-specific laws.	[47]
2	Impersonation attacks	Fingerprint biometrics.	[81,105]
		Elliptic curve cryptosystems.	[66,68,69]
		Hashing functions.	[56,67,70,77,87]
		Asymmetric encryption function.	[72]
		Mutual authentication.	[72,88]
		Use of random values like OTP.	[102,103]

Table 2. *Cont.*

S/No	Threat Models	Countermeasure	References
3	Replay attacks	Pairing-based cryptography and timestamp in encrypted data.	[66,68,69,102,103]
		Hashing functions.	[56,70]
		Use of one-time username.	[77]
4	Masquerade attack	Elliptic curve cryptosystem.	[66,68,69]
		Mutual authentication technique.	[72,88]
		Hash functions.	[56,67,70,71,77]
		Use of physiological and behavioural biometrics.	[78,80,81,89,105]
5	Spoofing attacks	Biometric authentication.	[68,80,81,89,104,105,107]
		Mutual authentication technique.	[72,88]
6	Social engineering attack	Multifactor authentication scheme, customer alert systems, antiphishing systems.	[108]
		Multidimensional approach, including technology, policies, procedures, standards, employee training, and awareness programs.	[109–111]
		Anomaly-based intrusion detection system to thwart SMS messaging attacks.	[112]
7	Phishing attacks	Multifactor authentication, anomaly-based intrusion detection system, email authentication, encryption, secure sockets layer, reports of suspicious activities, back-end analytics, user training/awareness, content-based filtering, blacklisting, and whitelisting.	[112–114]
		Using machine learning, profile matching, text mining, ontology, honeypots, and client–server authentication.	[115]
8	Trojan horse attacks	Integrating biometric and cryptography.	[68,69]
		Binary code obfuscation and hardware-based code attestation.	[116]
		Malware detection and prevention technique.	[106]
9	Eavesdropping attacks	Message authentication code (MAC).	[70]
		Use of ECIES and ECDSA.	[66]
10	Brute force attacks	Use of cryptographic hash functions.	[56,70,77,87]
11	Guessing attack	Elliptic curve cryptosystem.	[66–70]
		Password-salting mechanism.	[87]
		Hashing functions.	[56,77]
12	Shoulder surfing attack	Use of sightless multifactor authentication.	[79–81,85,86,89,90,105]
13	Man-in-the-middle (MITM) attack	Elliptic curve cryptosystem.	[66,69]
		Use of both biometric fingerprint and elliptic curve cryptosystem.	[68]
		Multifactor authentication.	[79,85,86,90]
		Symmetric encryption and message authentication code.	[56,67,70,71,73,74,76,102,103]
14	Salami attack	Defining an efficient and robust user and security policy that contains different privileges, updating security systems, initiating both SMS and email message alerting customers regarding any transaction that occurs, and advising the customers to report any unaware money reductions.	[18]

Table 2. *Cont.*

S/No	Threat Models	Countermeasure	References
15	Insider attacks	Using elliptic curve cryptography.	[66,68,70]
		Using identity-based cryptography.	[75]
		Certificate-based signcryption.	[117]
16	Denial of service (DoS) attacks	Cryptographic hash functions.	[56,67,68,70,71,77,87]
		Biometric fingerprint authentication.	[52,81,104,105]
	Distributed denial of service (DDoS) attacks	Nonlinear control approach that can prevent malicious attack packets.	[118]
		A hybrid intrusion detection system that uses both anomaly-based and signature-based detection methods.	[119]
17	Mobile phone theft	Remote device wipe, training customers, access blocking, data encryption, online or offline data backup, remote access to built-in cameras, GPS device tracking, and PIN protection.	[64]

5. Conclusions and Future Work

The advent of mobile money has enhanced the standard of living of the unbanked population in developing countries. As much as it offers a wide range of services and benefits, mobile money has experienced increases in attacks against the current 2FA scheme. This study conducted a review of the threat models and countermeasures in the 2FA scheme for mobile money. The authors utilised an appropriate search strategy to review the relevant literature.

With the comprehensive research and literature analysis, the threat models in the 2FA scheme for mobile money were classified into five categories: (1) attacks against privacy; (2) attacks against authentication, such as impersonation attack, replay attacks, masquerade attack, spoofing attacks, social engineering attack, phishing attack, and Trojan horse attacks; (3) attacks against confidentiality, such as eavesdropping attacks, brute force attacks, guessing attacks, and shoulder surfing attack; (4) attacks against integrity, such as MITM attack, salami attack, and insider attacks; (5) attacks against availability such as DoS and DDoS attacks, and mobile phone theft.

Furthermore, the countermeasures against the threat models in the 2FA scheme for mobile money were categorised into two, namely, cryptographic functions (such as asymmetric encryption function, symmetric encryption function, and hash function) and personal identification. Personal identification was subdivided into two categories: (1) number-based countermeasures such as password, PIN, OTP, and QR code; (2) biometric-based countermeasures, which was further classified into physiological biometrics (e.g., fingerprint recognition, face recognition, iris recognition, and retina recognition) and behavioural biometrics (e.g., voice recognition).

This work, therefore, will help MMSPs, decision-makers, and governments that wish to improve their current mobile money authentication method. Furthermore, it will help researchers who are doing an initial review of mobile money authentication schemes and mobile banking schemes. With a thorough analysis of the literature, we conclude that the current mobile money authentication system needs to be improved using a secure multifactor authentication scheme implementing a PIN, OTP, and biometric fingerprint. Moreover, data in transit and storage should be protected using end-to-end encryption and decryption techniques.

Author Contributions: Data curation, G.A.; formal analysis, M.A.D. and A.E.S.; investigation, G.A.; methodology, G.A.; supervision, M.A.D. and A.E.S.; writing—review and editing, G.A., M.A.D., and A.E.S. All authors read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors offer their heartfelt appreciation to the anonymous reviewers for their insightful suggestions and constructive comments. The authors extend their appreciations to Muni University and NM-AIST.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Suri, T. Mobile Money. *Annu. Rev. Econ.* **2017**, *9*, 497–520. [CrossRef]
2. Grundmann, A.S. Feasibility Study of a Mobile Payment System on Kasadaka: A Sustainable Voice Service Platform. Bachelor's Thesis, Vrije Universiteit, Amsterdam, The Netherlands, 2018.
3. Kanobe, F.; Alexander, M.P.; Bwalya, K.J. Information Security Management Scaffold for Mobile Money Systems in Uganda. In Proceedings of the 18th European Conference on Cyber Warfare & Security, University of Coimbra, Coimbra, Portugal, 4–5 July 2019; pp. 239–248.
4. Uganda Communications Commission (UCC). *Telecommunications, Broadcasting and Postal Markets Industry Report Q2 (April–June) 2019*; UCC: Kampala, Uganda, 2019. Available online: https://www.ucc.co.ug/wp-content/uploads/2017/09/Industry-Report-Q2-April-June-2019-Final.pdf (accessed on 18 June 2020).
5. Bank of Uganda (BoU). *Bank of Uganda (BoU) Annual Report-2018/19*; Bank of Uganda: Kampala, Uganda, 2019. Available online: https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/publications/Annual_Reports/All/Annual-Report-2019.pdf (accessed on 14 July 2020).
6. Okeleke, K. *Uganda: Driving Inclusive Socio-Economic Progress through Mobile-Enabled Digital Transformation*; GSM Association: London, UK, 2019; Available online: https://www.gsma.com (accessed on 20 May 2020).
7. Darvish, H.; Husain, M. Security Analysis of Mobile Money Applications on Android. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 3072–3078.
8. Ali, G.; Dida, M.A.; Sam, A.E. Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda. *Information* **2020**, *11*, 309. [CrossRef]
9. Gwahula, R. Risks and Barriers Associated with Mobile Money Transactions in Tanzania. *Bus. Manag. Strat.* **2016**, *7*, 121–139.
10. Musuva-Kigen, P.; Ekpeke, M.; Inkoom, E.; Inkoom, B.; Masesa, D.; Kaimba, B.; Mbae, K. *Kenya Cyber Security Report 2016*; Serianu Ltd.: Nairobi, Kenya, 2016.
11. Castle, S.; Pervaiz, F.; Weld, G.; Roesner, F.; Anderson, R. Let's talk money: Evaluating the security challenges of mobile money in the developing world. In Proceedings of the 7th Annual Symposium on Computing for Development (ACM DEV'16), New York, NY, USA, 18–20 November 2016; pp. 1–10.
12. Buku, M.; Mazer, R. Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System. 2017. Available online: http://www.cgap.org/publications/fraud-mobile-financial-services (accessed on 11 March 2020).
13. Lonie, S. Fraud Risk Management for Mobile Money: An Overview. 2017. Available online: https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf (accessed on 12 February 2020).
14. Bosamia, M.P. Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. In Proceedings of the 2017 International Conference on Soft Computing and Its Engineering Applications (icSoftComp-2017), Changa, India, 1–2 December 2017; pp. 1–7.
15. Maseno, E.M.; Ogao, P.; Matende, S. Vishing Attacks on Mobile Platform in Nairobi County Kenya. *Int. J. Adv. Res. Comput. Sci. Technol. IJARCST* **2017**, *5*, 73–77.
16. Akomea-Frimpong, I.; Andoh, C.; Akomea-Frimpong, A.; Dwomoh-Okudzeto, Y. Control of Fraud on Mobile money services in Ghana: An exploratory study. *J. Money Laund. Control* **2019**, *22*, 300–317. [CrossRef]
17. Balasubramanian, S. Study of Cybercrime in the Banking and Financial Sectors. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2018**, *3*, 1205–1212.
18. Alhassan, N.S.; Yusuf, M.O.; Karmanje, A.R.; Alam, M. Salami Attacks and their Mitigation—An Overview. In Proceedings of the 5th International Conference on Computing for Sustainable Global Development, New Delhi, India, 14–16 March 2018; pp. 4639–4642.
19. Kunda, D.; Chishimba, M. A Survey of Android Mobile Phone Authentication Schemes. *Mob. Netw. Appl.* **2018**, *73*, 1–9. [CrossRef]
20. Phipps, R.; Mare, S.; Ney, P.; Webster, J.; Heimerl, K. ThinSIM-Based Attacks on Mobile Money Systems. In Proceedings of the COMPASS '18: ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS), New York, NY, USA, 20–22 June 2018; pp. 1–11.

21. Talom, F.S.G.; Tengeh, R.K. The Impact of Mobile Money on the Financial Performance of the SMEs in Douala, Cameroon. *Sustainability* **2019**, *12*, 183. [CrossRef]
22. Saxena, S.; Vyas, S.; Kumar, B.S.; Gupta, S. Survey on Online Electronic Payments Security. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, UAE, 4–6 February 2019; pp. 746–751.
23. Reaves, B.; Bowers, J.; Scaife, N.; Bates, A.; Bhartiya, A.; Traynor, P.; Butler, K.R.B. Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications. *ACM Trans. Priv. Secur.* **2017**, *20*, 1–31. [CrossRef]
24. Maina, J. *Data Protection in Mobile Money*; GSMA: London, UK, 2019.
25. GSMA. *The Mobile Economy Sub-Saharan Africa 2018*; GSMA: London, UK, 2018.
26. Nair, S.; Khatri, S.K.; Gupta, H. A Model to Enhance Security of Digital Transaction. In Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019; pp. 17–21.
27. Ferrag, M.A.; Maglaras, L.; Derhab, A.; Janicke, H. Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommun. Syst.* **2020**, *73*, 1–32. [CrossRef]
28. Han, D.; Chen, Y.; Li, T.; Zhang, R.; Zhang, Y.; Hedgpeth, T. Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), New Delhi, India, 29 October–2 November 2018; pp. 401–415.
29. Dmitrienko, A.; Liebchen, C.; Rossow, C.; Sadeghi, A.-R. On the (In)Security of Mobile Two-Factor Authentication. In Proceedings of the 2014 International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; FC 2014, LNCS 8437. Springer: Berlin/Heidelberg, Germany, 2014; pp. 365–383.
30. Promontory. *Biometric Authentication in Payments: Considerations for Policymakers*; Promontory Financial Group: Washington, DC, USA, 2017.
31. Hayikader, S.; Hanis, F.N.; Ibrahim, J. Issues and Security Measures of Mobile Banking Apps. *Int. J. Sci. Res. Publ.* **2016**, *6*, 36–41.
32. Rouse, M. Single-Factor Authentication (SFA). 2017. Available online: https://searchsecurity.techtarget.com/ (accessed on 1 May 2020).
33. Rahav, A. The Secret Security Wiki. 2018. Available online: https://doubleoctopus.com/security-wiki/authentication/single-factor-authentication/ (accessed on 4 May 2020).
34. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [CrossRef]
35. Bissada, A.; Olmsted, A. Mobile multi-factor authentication. In Proceedings of the 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 210–211.
36. Australian Cyber Security Centre (ACSC). Implementing Multi-Factor Authentication. 2019. Available online: https://www.acsc.gov.au/ (accessed on 22 May 2020).
37. Hamilton, C.; Olmstead, A. Database multi-factor authentication via pluggable authentication modules. In Proceedings of the 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 367–368.
38. Pareek, A.; Khandaker, E. *Building an In-House Mobile Money Platform (UNCDF)*; UN Capital Development Fund: New York, NY, USA, 2018.
39. Nyamtiga, B.W.; Sam, A.; Laizer, L.S. Security Perspectives for USSD versus SMS in Conducting Mobile Transactions: A Case Study of Tanzania. *Int. J. Technol. Enhanc. Emerg. Eng. Res.* **2013**, *1*, 38–43.
40. McGrath, F.; Lonie, S. *Platforms for Successful Mobile Money Services*; GSMA: London, UK, 2013.
41. Nyaketcho, D.; Lindskog, D.; Ruhl, R. *STK Implementation in SMS Banking in M-Pesa—Kenya, Exploits and Feasible Solutions*; Concordia: St. Louis, MO, USA, 2017.
42. GSMA. *First Steps for Mitigating Simjacker-Related Risks Right Now*; GSMA: London, UK, 2019.
43. Saxena, N.; Payal, A. Enhancing Security System of Short Message Service for M-Commerce in GSM. *Int. J. Comput. Sci. Eng. Technol. IJCSET* **2011**, *2*, 127–133.
44. Mahajan, R.; Saran, J.; Rajagopalan, A. *Mitigating Emerging Fraud Risks in the Mobile Money Industry*; Deloitte: Mumbai, India, 2015.
45. Schneier, B. Two-Factor Authentication: Too Little, Too Late. *Commun. ACM* **2005**, *48*, 1. [CrossRef]

46. Liu, F. Efficient Two-Factor Authentication Protocol Using Password and Smart Card. *J. Comput.* **2013**, *8*, 3257–3263. [CrossRef]
47. Makulilo, A.B. Privacy in mobile money: Central banks in Africa and their regulatory limits. *Int. J. Law Inf. Technol.* **2015**, *23*, 372–391. [CrossRef]
48. Harris, A.; Goodman, S.; Traynor, P. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Wash. J. Law Technol. Arts* **2013**, *8*, 1–20.
49. McKee, K.; Kaffenberger, M.; Zimmerman, J. Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks. 2015. Available online: https://www.cgap.org/sites/default/files/researches/documents/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf (accessed on 13 July 2020).
50. Gilman, L.; Joyce, M. Managing the Risk of Fraud in Mobile Money. 2012. Available online: http://www.gsma.com/mmu (accessed on 28 February 2020).
51. Mudiri, J.L. *Fraud in Mobile Financial Services*; MicroSave: New Delhi, India, 2012.
52. Mtaho, A.B. Improving Mobile Money Security with Two-Factor Authentication. *Int. J. Comput. Appl.* **2015**, *109*, 9–15.
53. Paik, M. Stragglers of the herd get eaten: Security concerns for GSM mobile banking applications. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, New York, NY, USA, 22–23 February 2010.
54. Nyamtiga, B.W.; Anael, S.; Loserian, L.S. Enhanced Security Model for Mobile Banking Systems in Tanzania. *Int. J. Technol. Enhanc. Emerg. Eng. Res.* **2013**, *1*, 4–19.
55. Mtaho, A.B.; Mselle, L. Securing Mobile money services in Tanzania: A Case of Vodacom M-Pesa. *Int. J. Comput. Sci. Netw. Solut.* **2014**, *2*, 1–11.
56. Brinzel, R.; Anita, C.; Shraddha, M. Two-Factor Verification using QR-code: A unique authentication system for Android Smartphone users. In Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (ic3i), Noida, India, 14–17 December 2016; pp. 457–462.
57. Aloul, F.; Zahidi, S.; El-Hajj, W. Two-Factor authentication using mobile phones. In Proceedings of the 2009 IEEE/ACS International Conference on Computer Systems and Applications, Rabat, Morocco, 10–13 May 2009; pp. 641–644.
58. Jarecki, S.; Krawczyk, H.; Shirvanian, M.; Saxena, N. Two-Factor Authentication with End-to-End Password Security. In Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC), Rio De Janeiro, Brazil, 25–29 March 2018; pp. 431–461.
59. Kaur, S.; Sharma, S.; Singh, A. Cyber Security: Attacks, Implications, and Legitimations across the Globe. *Int. J. Comput. Appl.* **2015**, *114*, 21–23. [CrossRef]
60. Sadekin, S.M.; Shaikh, H.M. Security of E-Banking in Bangladesh. *J. Financ. Account.* **2016**, *4*, 1–8. [CrossRef]
61. Altwairqi, A.F.; AlZain, M.A.; Soh, B.; Masud, M.; Al-Amri, J. Four Most Famous Cyber Attacks for Financial Gains. *Int. J. Eng. Adv. Technol. IJEAT* **2019**, *9*, 2131–2139.
62. Trulioo. Emerging Fraud Risk in the Mobile Wallet Ecosystem. 2015. Available online: https://www.trulioo.com/blog/emerging-fraud-risk-in-the-mobile-wallet-ecosystem/ (accessed on 14 March 2020).
63. Mutong'Wa, S.M.; Khaemba, S.W. A comparative study of critical success factors (CSFS) in the implementation of mobile money transfer services in Kenya. *Eur. J. Eng. Technol.* **2014**, *2*, 8–31.
64. Tu, Z.; Turel, O.; Yuan, Y.; Archer, N. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Inf. Manag.* **2015**, *52*, 506–517. [CrossRef]
65. Barker, E.; Barker, C.W. *Recommendation for Key Management: Part 2—Best Practices for Key Management Organizations*; NIST Special Publication 800-57, Rev. 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
66. Bojjagani, S.; Sastry, V.N. SSMBP: A Secure SMS-based Mobile Banking Protocol with Formal Verification. In Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, UAE, 19–21 October 2015; pp. 252–259.
67. Kisore, N.R.; Sagi, S. A secure SMS protocol for implementing the digital cash system. In Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 10–13 August 2015; pp. 1883–1892.
68. Ray, S.; Biswas, G.P.; Dasgupta, M. Secure Multi-Purpose Mobile-Banking Using Elliptic Curve Cryptography. *Wirel. Pers. Commun.* **2016**, *90*, 1331–1354. [CrossRef]

69. Shilpa, S.; Panchami, V. BISC Authentication Algorithm: An Efficient New Authentication Algorithm Using Three-Factor Authentication for Mobile Banking. In Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 19 November 2016; pp. 1–5.
70. Salim, A.; Sagheer, A.; Yaseen, L. Design and Implementation of a Secure Mobile Banking System Based on Elliptic Curve Integrated Encryption Schema. In Proceedings of the Communications in Computer and Information Science, Gdańsk, Poland, 23–24 June 2020; Springer Nature: Cham, Switzerland, 2020; pp. 424–438.
71. Sharma, N.; Bohra, B. Enhancing online banking authentication using the hybrid cryptographic method. In Proceedings of the 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, India, 9–10 February 2017; pp. 1–8.
72. Purnomo, A.T.; Gondokaryono, Y.S.; Kim, C.-S. Mutual authentication in securing a mobile payment system using encrypted QR code based on Public Key Infrastructure. In Proceedings of the 6th International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, 3–4 October 2016; pp. 194–198.
73. Mitra, S.; Jana, B.; Poray, J. Implementation of a Novel Security Technique Using Triple-DES in Cashless Transaction. In Proceedings of the 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, India, 22–23 December 2017; pp. 1–6.
74. Hu, J.-Y.; Sueng, C.-C.; Liao, W.-H.; Ho, C.C. Android-Based mobile payment service protected by 3-factor authentication and virtual private ad hoc networking. In Proceedings of the 2012 Computing, Communications and Applications Conference, Hong Kong, China, 11–13 January 2012; pp. 111–116.
75. Alornyo, S.; Mireku, K.K.; Tonny-Hagan, A.; Hu, X. Mobile Money Wallet Security against Insider Attack Using ID-Based Cryptographic Primitive with Equality Test. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019; pp. 82–87.
76. Zhang, X.; Zeng, H.; Zhang, X. Mobile payment protocol based on dynamic mobile phone token. In Proceedings of the IEEE 9th International Conference on Communication Software and Networks (ICCSN), Guangzhou, China, 6–8 May 2017; pp. 680–685.
77. Alhothailya, A.; Alrawaisa, A.; Hua, C.; Lie, W. One-Time-Username: A Threshold-Based Authentication System. In Proceedings of the International Conference on Identification, Information and Knowledge in the Internet of Things, Qufu, China, 19–21 October 2017; pp. 426–432.
78. Coneland, R.; Crespi, N. Wallet-On-Wheels—Using a vehicle's identity for secure mobile money. In Proceedings of the 17th International Conference on Intelligence in Next Generation Networks (ICIN), Venice, Italy, 15–16 October 2013; pp. 102–109.
79. Akoramurthy, B.; Arthi, J. GeoMoB—A Geo Location based browser for secured Mobile Banking. In Proceedings of the IEEE Eighth International Conference on Advanced Computing (ICoAC), Chennai, India, 19–21 January 2017; pp. 83–88.
80. Chetalam, J.L. Enhancing Security of MPesa Transactions by Use of Voice Biometrics. Master's Thesis, United States of International University, Nairobi, Kenya, 2018.
81. Sharma, L.; Mathuria, M. Mobile banking transaction using fingerprint authentication. In Proceedings of the 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 1300–1305.
82. Wimberly, H.; Liebrock, L.M. Using Fingerprint Authentication to Reduce System Security: An Empirical Study. In Proceedings of the 2011 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 22–25 May 2011; pp. 32–46.
83. Hao-Jun, X.; Wei-Chi, K.; Yu-Xuan, D. An Observation Attacks Resistant PIN-Entry Scheme Using Localized Haptic Feedback. In Proceedings of the 2016 IEEE Region 10 Symposium (TENSYMP), Bali, Indonesia, 9–11 May 2016; pp. 59–64.
84. Bultel, X.; Dreier, J.; Giraud, M.; Izaute, M.; Kheyrkhah, T.; Lafourcade, P.; Mot'a, L. Security Analysis and Psychological Study of Authentication Methods with PIN Codes. In Proceedings of the 12th International Conference on Research Challenges in Information Science (RCIS), Nantes, France, 29–31 May 2018; pp. 1–11.
85. Islam, M.S. An algorithm for electronic money transaction security (Three Layer Security): A new approach. *Int. J. Secur. Appl.* **2015**, *9*, 203–214. [CrossRef]
86. Ombiro, Z.B.H. Mobile-Based Multi-Factor Authentication Scheme for Mobile Banking. Master's Thesis, University of Nairobi, Nairobi, Kenya, 2016.

87. Singh, B.; Jasmine, K.S. Secure End-To-End Authentication for Mobile Banking. In *Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2015; Volume 349, pp. 223–232.
88. Fan, K.; Li, H.; Jiang, W.; Xiao, C.; Yang, Y. U2F based secure mutual authentication protocol for mobile payment. In Proceedings of the ACM Turing 50th Celebration Conference, Shanghai, China, 12–14 May 2017; pp. 1–6.
89. Islam, I.; Munim, K.M.; Islam, M.N.; Karim, M.M. A Proposed Secure Mobile Money Transfer System for SME in Bangladesh: An Industry 4.0 Perspective. In Proceedings of the 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 24–25 December 2019; pp. 1–6.
90. Zadeh, M.J.; Barati, H. Security Improvement in Mobile Banking Using Hybrid Authentication. In Proceedings of the 3rd International Conference on Advances in Artificial Intelligence, Istanbul, Turkey, 26–28 October 2019; pp. 198–201.
91. Kasat, O.K.; Bhadade, U.S. Revolving Flywheel PIN Entry Method to Prevent Shoulder Surfing Attacks. In Proceedings of the 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; pp. 1–5.
92. Elganzoury, H.S.; Abdulhafez, A.A.; Hegazy, A.A. A Provably Secure Android-Based Mobile Banking Protocol. *Int. J. Secur. Appl.* **2017**, *11*, 77–88. [CrossRef]
93. Verma, A.; Brar, R.; Ummat, A. Cloud Computing and Homomorphic Encryption. *Int. J. Comput. Sci. Inf. Secur. IJCSIS* **2017**, *15*, 47–55.
94. Venkatesh, G.; Gopal, S.V.; Meduri, M.; Sindhu, C. Application of Session Login and One Time Password in Fund Transfer System Using RSA Algorithm. In Proceedings of the International Conference on Electronics, Communication, and Aerospace Technology ICECA 2017, Coimbatore, India, 20–22 April 2017; pp. 732–738.
95. Srivastava, S.; Sivasankar, M. On the generation of alphanumeric one time passwords. In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–27 August 2016; pp. 1–3.
96. Prasad, K.; Aithal, P.S. A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *Int. J. Adv. Trends Eng. Technol.* **2018**, *3*, 1–11.
97. Soare, C.A. Internet Banking Two-Factor Authentication using Smartphones. *J. Mob. Embed. Distrib. Syst.* **2012**, *4*, 12–18.
98. Iftikhar, J.; Hussain, S.; Mansoor, K.; Ali, Z.; Chaudhry, S.A. Symmetric-Key Multi-Factor Biometric Authentication Scheme. In Proceedings of the 2nd International Conference on Communication, Computing and Digital Systems (C-CODE), Islamabad, Pakistan, 6–7 March 2019; pp. 288–292.
99. Surekha, A.; Anand, P.M.R.; Indu, I. E-Payment Transactions Using Encrypted QR Codes. *Int. J. Appl. Eng. Res.* **2015**, *10*, 460–463.
100. Ugwu, C.; Mesigo, T. A Novel Mobile Wallet Based on Android OS and Quick Response Code Technology. *Int. J. Adv. Res. Comput. Sci. Technol. IJARCST* **2015**, *3*, 85–89.
101. Ruslan, M.K.; Gusti, S.; Yudi, F.; Anderes, G. QR Code Payment in Indonesia and Its Application on Mobile Banking. In Proceedings of the FGIC 2nd Conference on Governance and Integrity, Yayasan Pahang, Malaysia, 19–20 August 2019; pp. 551–568.
102. Tandon, A.; Sharma, R.; Sodhiya, S.; Vincent, P.D. QR Code-based secure OTP distribution scheme for Authentication in Net-Banking. *Int. J. Eng. Technol. IJET* **2013**, *5*, 2502–2505.
103. Ximenes, A.M.; Sukaridhoto, S.; Sudarsono, A.; Albaab, M.R.; Basri, H.; Yani, M.A.; Islam, E. Implementation QR Code Biometric Authentication for Online Payment. In Proceedings of the 2019 International Electronics Symposium (IES), Surabaya, Indonesia, 27–28 September 2019; pp. 676–682.
104. Ahsan, K.; Iqbal, S.; Hussain, M.A.; Nadeem, A. A Mobile Payment Model Using Biometric Technology. *Int. J. Adv. Sci. Eng. Technol.* **2016**, *4*, 17–20.
105. Okpara, O.S.; Bekaroo, G. Cam-Wallet: Fingerprint-Based authentication in M-wallets using embedded cameras. In Proceedings of the 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Milan, Italy, 6–9 June 2017; pp. 1–5.
106. Bosamia, M.; Patel, D. Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *Int. J. Comput. Sci. Eng.* **2019**, *7*, 810–817. [CrossRef]

107. Fujii, H.; Tsuruoka, Y. SV-2FA: Two-Factor User Authentication with SMS and Voiceprint Challenge-Response. In Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), London, UK, 9–12 December 2013; pp. 283–287.
108. Airehrour, D.; Nair, N.V.; Madanian, S. Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information* **2018**, *9*, 110. [CrossRef]
109. Luo, X.; Brody, R.; Seazzu, A.; Burd, S. Social Engineering: The Neglected Human Factor for Information Security Management. *Inf. Resour. Manag. J.* **2011**, *3*, 1–8. [CrossRef]
110. Chinta, M.; Alaparthi, J.; Koda, E. A Study on Social Engineering Attacks and Defence Mechanisms. *Int. J. Comput. Sci. Inf. Secur. IJCSIS* **2016**, *14*, 225–231.
111. Conteh, N.Y.; Schmick, P.J. Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 31–38. [CrossRef]
112. Hamandi, K.; Salman, A.; Elhajj, I.H.; Chehab, A.; Kayssi, A. Messaging Attacks on Android: Vulnerabilities and Intrusion Detection. *Mob. Inf. Syst.* **2015**, 1–13. [CrossRef]
113. Shahriar, H.; Klintic, T.; Clincy, V. Mobile Phishing Attacks and Mitigation Techniques. *J. Inf. Secur.* **2015**, *6*, 206–212. [CrossRef]
114. Singh, L.J.; Imphal, N. A Survey on Phishing and Anti-Phishing Techniques. *Int. J. Comput. Sci. Trends Technol. IJCST* **2018**, *6*, 62–68.
115. Aleroud, A.; Zhou, L. Phishing environments, techniques, and countermeasures: A survey. *Comput. Secur.* **2017**, *68*, 160–196. [CrossRef]
116. Jung, J.-H.; Kim, J.Y.; Lee, H.-C.; Yi, J.H. Repackaging Attack on Android Banking Applications and Its Countermeasures. *Wirel. Pers. Commun.* **2013**, *73*, 1421–1437. [CrossRef]
117. Lu, Y.; Li, J. Efficient Certificate-Based Signcryption Secure against Public Key Replacement Attacks and Insider Attacks. *Sci. World J.* **2014**, *2014*, 295419. [CrossRef]
118. Li, M.; Li, M. An Adaptive Approach for Defending against DDoS Attacks. *Math. Probl. Eng.* **2010**, *2010*, 570940. [CrossRef]
119. Cepheli, Ö.; Büyükçorak, S.; Kurt, G.K. Hybrid Intrusion Detection System for DDoS Attacks. *J. Electr. Comput. Eng.* **2016**, *2016*, 1075648. [CrossRef]