International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Mobile Payment (SMP): Challenges and Potential Solutions.

Shahad AL-Tamimi [1], Qasem Abu Al-Haija *[2]

Submitted: 04/11/2023 **Revised**: 23/12/2023 **Accepted**: 05/01/2024

Abstract: Mobile devices, in particular, have revolutionized how financial transactions are conducted, making secure mobile payment (SMP) a primary method for completing transactions. The intersection of finance and technology, facilitated by internet usage, has given rise to digital payment systems, which serve as the foundation for financial inclusion. However, the convenience of mobile payment also brings forth several security issues that need to be addressed. Near Field Communication (NFC) technology has significantly impacted consumers' lives by integrating with mobile payment systems. Consequently, NFC-enabled payment systems have recently emerged in the consumer market, attracting the interest of businesses seeking to invest in this technology. This study comprehensively examines the mobile payment security landscape, encompassing security challenges and proposed solutions. Through this review, we aim to contribute to understanding mobile payment security and foster advancements that ensure a secure and reliable payment ecosystem.

Keywords: *Mobile Payment (MP), Secure Mobile Payment (SMP), Online Payment, Mobile Devices, Financial Transaction, Electronic Transaction, Digital Payment Systems (DPS), Digital Environment, Near Field Communication (NFC).*

1. Introduction

The Mobile Payment Forum I states that mobile payment (MP) is "a transaction between two individuals for specific goods or services, using a handheld equipment as a carrier, and an economical operation carried out over a mobile communication network." [1]. Thus, MP is described as processing payments via mobile devices, for instance, mobile devices, smartwatches, and any NFC-enabled device. It also qualifies as a financial procedure involving mobile digital interaction devices to start, approve, and finalize financial transactions. A business activity accomplished with a computing device connected to a mobile network is defined as a satisfied economic transaction [2]. NFC is a wireless technology with a short range that allows data transfer among devices close to one another [3] because of the integration of NFC. Thus, NFC technology allows the integration of services from various applications into one mobile device. NFC technology has grown in popularity over the last decade due to the increased need for wireless automation. Most automation has focused on data sharing and access control, especially contactless payment technologies [4]. Mobile device technology and contactless mobile transactions have gained popularity during the past ten years. In all likelihood, MP is regarded as more secure than regular credit card payments due to the extra security integrated into the mobile app.

There are various elements to consider while evaluating a payment system: authentication, encryption, and fraud detection [5].

Authentication is required to ensure authorized people access the

payment feature. Strong and multifactor authentication mechanisms, such as fingerprint or face recognition, must be used in a system. Conversely, encryption guarantees that payment-related data, especially financial card numbers and account information, is safely stored and communicated across the network [6]. Lastly, a successful payment method must contain risk management capabilities, including fraud detection and prevention, to detect and prevent suspicious activities such as money laundering [7]. This review article examines the technological underpinnings, benefits, problems, and prospects of secure mobile payment systems. It details the different security mechanisms. These systems employ encryption, tokenization, and biometric authentication. Furthermore, the article investigates the ease and adaptability of using secure mobile payment, its influence on financial transactions, and particularly the constraints involved with its broad implementation.

This study provides an inclusive overview of secure mobile payment (SMP) and its implications in the digital ecosystem, incorporating current research and industry developments. We explore the technical aspects of SMP systems, their transformative impacts on various divisions, and the latest inclinations and initiatives. This investigation aims to contribute to the insight and adoption of secure and convenient digital transactions. This paper is structured and organized to analyze SMP systematically. In Section 1, we dive into the underlying concept of SMP, forming a solid base for the succeeding sections. Section 2 is a perceptive

[1] *Department of Cybersecurity, King Hussein School of Computing Sciences, Prince Sumaya University for Technology, PO Box 1438, Amman 11941, Jordan*
ORCID ID: 0009-0005-327-8200
[2] *Department of Cybersecurity, Faculty of Computer & Information Technology, Jordan University of Science and Technology, PO Box 3030, Irbid 22110, Jordan.*
ORCID ID: 0000-0003-2422-0297
**Corresponding Author Email: qsabuhaija@just.edu.jo*

background section, offering an appropriate understanding of the subject matter. Section 3 reviews the research efforts commenced in previous findings over the last few years, providing an ample summary of the existing body of knowledge. Section 4 addresses the pressing concerns of SMP's attacks, threats, and security challenges. Within our results section, we propose new solutions to mitigate these risks. Finally, in Section 5, we draw meaningful conclusions summarizing our findings and contributions to the field, ensuring a consistent and impactful conclusion to this work.

2. Background

This section provides a comprehensive review of the concept of SMP processes involving diverse aspects such as digital payments, mobile payment categories, and models. By investigating these significant factors, we aim to present an unblemished understanding of the intricacies and distinctions in ensuring secure and reliable MP transactions.

2.1. Digital Payment Systems

Operating system platforms, including Android and iOS, have gained popularity in recent years thanks to the rise of devices and desktop computers. Peer-to-peer (P2P) transfers of money have advanced to the next stage of development with the introduction of Mobile Wallets and the development of Mobile Banking. These allow for many functions, such as bill payment and cash transfers, including payouts, ticket booking, smartphone recharges, and P2P money transfers. NFC digitally delivers money through the payer's financial institution into the payee's bank [8, 9]. While delivered via a contactless payment terminal during card emulation mode, a contactless card with low-power technology that allows devices to interact at a few millimeters can function like a smart card. Payments at the point of sale (POS) are one of the key use cases for this method, which is growing in importance given the pivotal role, ubiquity, and networking capabilities of mobile phones. Nevertheless, despite these benefits and the fact that the underlying NFC technology has been publicly available for some years, there has yet to be a globally established pay-with-your-phone mechanism [10].

2.2. Mobile Payment Categories

We have several categories or classifications of MP. Where Figure 2 shows the categories of mobile payment. Point of sales (POS): A payment mechanism that handles contact and contactless NFC transactions. Through a secure channel (TLS), the POS discusses with the issuing bank, where online payment is used to communicate between the POS and the issuing bank. [11,12]

2.2.1 Payment at the POS

This technology enables customers to pay with their cell phones.

Most of these solutions, particularly Apple Pay and Google Wallet, rely on integrated NFC technology. Hold the phone across an NFC-enabled station to use the embedded monetary system to create a connection. Subsequently, unlock your mobile device by double-clicking the main button or pressing your finger on the screen. Over the sensor for fingerprints to confirm the purchase. This secured component (SC) chip validates the transaction. This chip sends authorization again via the NFC modem; thus, the transaction is completed like a standard credit card swipe. The terminal transmits to the card operator or the merchant's ID number, card details, and transaction amount.

After reading the information, the processor sends a validation request to the card issuing bank. The card provided by the bank subsequently investigated fraud and determined whether the card was sufficient for paying the purchase amount. It either accepts or rejects the transaction. The merchant is subsequently alerted whether or not the transaction was accepted; these processes' built-in payment methods are simple to configure on a mobile device. [12,13]

2.2.2 Mobile Payment as the POS

This technology enables a merchant to utilize a mobile device and accept card payments. This approach often necessitates the download of a mobile app to a mobile device as well as the connection of the reader for the credit card to the mobile device. The installation is simple, quick, and convenient. It can accept card payments at any moment and anywhere in the world. Square Register (SR) is a prime instance of MP at the POS. SR enables both credit card reader purchases and keyed-in purchases. Currently, three types of credit card readers are acceptable: the square reader for magnetic stripe cards, the square reader over EMV chip cards, and the Square contactless and chip reader. The Square contactless and chip reader accepts NFC payments, which include Apple Pay. PayPal also offers comparable services.[10]

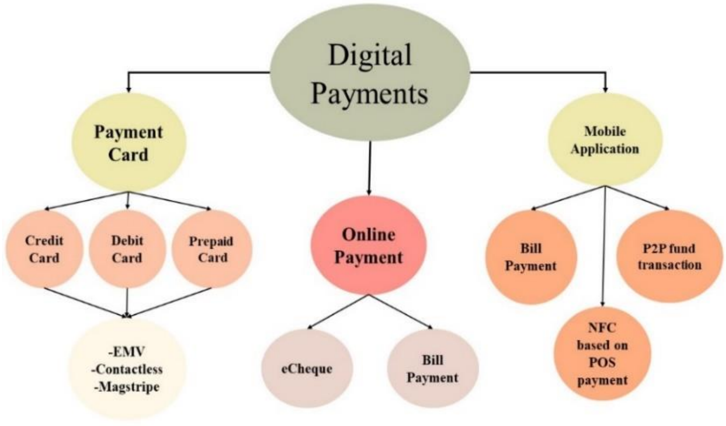

Fig. 1. Digital Payment [30].

2.2.3 Mobile Payment Platform

This approach allows customers to pay online using a mobile device. It necessitates installing and downloading a mobile app onto a mobile device. This approach can also be employed as a mobile wallet for POS payment. A bank account or a credit/debit card account is typically necessary for a connection to an MP account.

2.2.4 Independent Mobile Payment System

This approach offers MP capabilities comparable to MP platforms. A corporation may build its online payment service to serve mobile devices. These are known as independent MP systems. Amazon, Starbucks, and other companies' mobile applications are examples of these separate mobile payment systems.

2.2.5 Direct Carrier Billing

Customers can utilize their mobile devices to purchase items or services utilizing this approach. It is unable to accept credit or debit cards as payment. The purchase shall be added to the mobile subscriber's monthly phone bill. Typically, direct carrier billing entails charging by SMS texts. To complete purchases on a website, a user inputs their cell phone number. A text message with a transaction code is sent to the user. To complete the transaction, the consumer enters a code on the website.

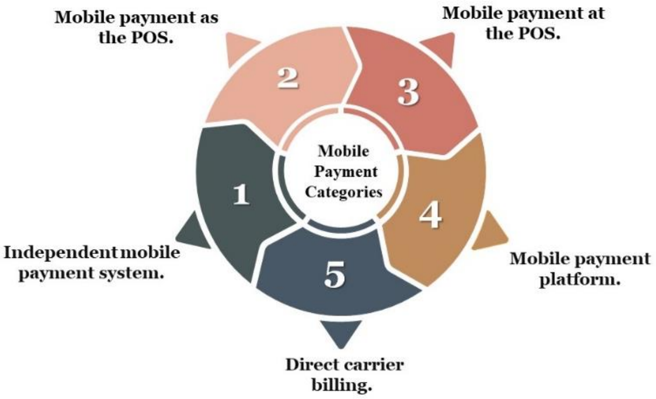
Mobile payment as the POS.
Mobile payment at the POS.
2
3
1
Mobile Payment Categories
4
5
Independent mobile payment system.
Mobile payment platform.
Direct carrier billing.

Fig. 2. Mobile Payment Categories.

2.3. Mobile Payment System

This system consists of several parts such as a mobile network, information technology (IT administrator) and user, financial institutions (bank), base transceiver station (BTS), and databases; thus, servers (telecom gateway servers such as short messaging service gateway (SMSGW) & USSD), core servers, and web servers). It then connects to multiple mobile network operators (MNO), essential elements to access the global mobile network. Communications (GSM) technology. The infrastructure is not a standalone entity; additional platforms give full commercial capabilities. Internal MNO interfaces include the SMS Centre (SMSC), USSD Gateway, Airtime In/Out Mediation Platform, Web Services, and Interactive Voice Response (IVR) Gateway. The outside interfaces consist of point-of-sale systems, biller systems, and payment system architecture, as shown in Figure 3.[1]

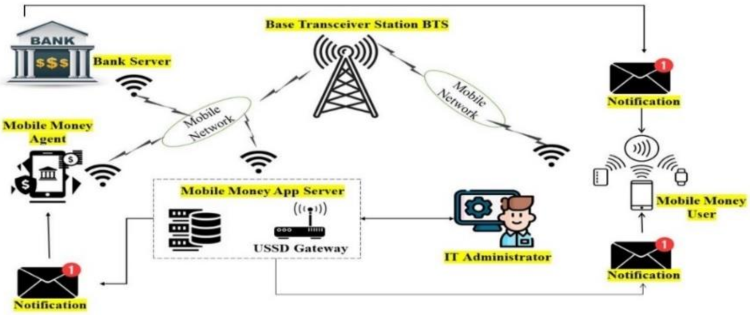

Fig. 3. Mobile Payment System Architecture (MPS) [14].

2.4. Mobile Payment Models

Mobile payment methods are typically designed to resist malware and ransomware attacks [15]. Figure 4 illustrates the four main payment models in secure mobile payments: QR-code payment, contactless payments, mobile wallets, and MP-based SMS. Each model represents a distinct approach to facilitating secure and convenient mobile transactions. By examining these models, we gain valuable insights into the diverse options available to consumers and businesses in the mobile payment landscape.

2.4.1 QR Code Payment

QR stands for Quick Response Code. The corresponding code is generated wirelessly and is used to make payments. These are currently a popular payment method, especially for contactless purchases. This is utilized when money must be deducted and must be credited. Both the merchant and the customer may use it. This can be considered a feature of mobile payment software that allows for frequent transactions. These can be utilized when the merchant generates the QR code and the amount details. This is considered useful for the customer to correct the payment details while the quantity is transferred.

2.4.2 Payments Through Contactless

NFC Thought is among the most essential and well-known contactless payment techniques. It involves a connection following rules and regulations that allow two devices to save, exchange, and transport data. The range is limited; it would likely work with limited capabilities like air dropping or Bluetooth characteristics to transmit data between many devices that must first be linked. The transaction can be completed successfully if the NFC-capable device is close to the user's device. Users favor NFC over other payment methods since the data is fully protected and incredibly simple. The secure website requires PIN authentication. Currently, bitcoin is also a contactless payment method [16].

2.4.3 Mobile Wallets

Mobile wallets are profit devices that complete transactions with a single click. The wallets are linked to the accounts, and money may be quickly moved through the bank account to the electronic wallets. Money can be given or received in return whenever a transaction requires a wallet for products and services like Apple Pay, Google Pay, and PayPal.

2.4.4 MP Based on SMS

The following payment technique is incredibly simple and user-friendly. It can be quick payment technical processes. There are certain drawbacks to this method of payment, for instance, the need for more user identity and the restriction on authenticity.

3. Related Works

MP has evolved into a crucial component of e-commerce. As a result, maintaining information confidentiality within the payment process is critical [17]. This section will discuss research findings and past studies on secure mobile payment. Table 1 will be reviewed carefully in detail. In Table 1, we cited the important studies for our research in the last eight years. Some studies discuss security threats and challenges facing MP; conversely, a study discusses both NFC and security challenges.

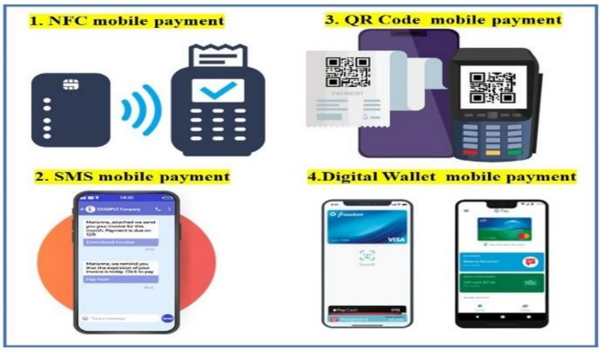

Fig. 4. Mobile Payment Models [8].

Where authors in [18] reviewed 92 papers from 2006 to 2021, the assessment results grouped Payment techniques in the digital age within four different payment modes: card payments, e-payments, MP, and cryptocurrency. The taxonomies of upcoming digital payment technologies give an overview of the widely scattered information on digital payment systems. As a result, the study gives insights into the most recent developments in digital payment technology and enhances digital finance learning. The categorization can also assist future scholars in obtaining high-quality references for their research on cashless payment systems. In [19], the author recommended a conceptual framework for investigating the relationship between key personality factors and consumers' online buying patterns. Personalized consumer profiles are produced using the TIPI test, a viable and tested alternative to the Five-Factor model. The findings link major personality factors and various online purchasing functions. While in [20 distinct e-shop functions are chosen by specific user groups. The machine learning technique considers data as unanticipated factors, primarily concerned with prediction rather than inference to anticipate unseen consequences or future behavior. Knowing the consumer’s risk perception and employing Machine Learning approaches to forecast users’ preferences allows you to maximize specific aspects of e-commerce. However, in [21], they reviewed 32 papers from 2012 to 2021. This application offers an NFC-based Established Protocol to Earn Mobile Transaction (NSPMT) protocol utilizing the defense within the depth approach. A comprehensive defense method comprises three stages: hardware protection, application defense, and communication security. They suggested that protocol consumes less power, has lower communication costs, and has a lower computing cost than previous efforts, which can improve the overall power consumption [28].

Moreover,[21] reviewed 26 papers from 2004 to 2020. The authors of this research study have identified several benefits, dangers, and issues linked with MP. The authors also proposed security procedures and preventions implemented by stakeholders to ensure the payment network's secure operation. Since traditional systems and PIN functionality have compromised user data, the authors propose a biometric system to recognize the authorized user. Problems with MP and security may be minimized by using biometric technology systems for all data safety and completing transactions regularly. With the use and assistance of advancing technology, the payment method will also be an immediate enhancement.

Also [29], the authors discussed alternative payment formats, the use of this technology, and the given security features. Also, this paper represents an overview and discussion of different components of SMP structure and limitations, mainly focusing on security and privacy, confidentiality, authentication, and scalability [30]. Thus, in [24], they review 83 papers from 2003 to 2019. The researcher in this study classifies MP into two categories: firstly, TCP (third-party payment company)-led MP, and secondly, bank-led MP. Which two categories are based on the architecture of MP? A variety of perspectives identify mobile payments differently. Mobile payments are classified into two types based on their distance: near-field payments and distant payments. It is classified as offline payment or online payment based on the connection of the user's mobile terminal.

Furthermore, contributors of [23] reviewed 43 papers from 2011 to 2020. In this study, they presented a comparison between their suggested structure and the other three existing systems. Based on these criteria, they recommended an encrypted electronic payment method for e-commerce settings. The suggested technique is a proxy for communicating between the client/merchant and the bank. The security study revealed that the suggested approach provides superior protection concerning information confidentiality, nonrepudiation, integrity, availability, and anonymity. This article will be expanded to demonstrate the use of our proposed framework in practical applications by demonstrating its ability to prevent numerous assaults and predict the time required for electronic payment. However, in [25], the research of this study, they review 39 papers. They created a (Read Only NFC) **RONFC** initial prototype for a common mobile contactless payment circumstance. They demonstrated through performance assessments that the suggested approach promises to satisfy the expectations for regular NFC-based MP while meeting their requirements for security. Developments in technology over the past decade have rendered it a popular alternative to many types of mobile transactions, especially in the MP business. Hundreds of NFC-enabled mobile devices are available today, with millions of people utilizing them. If they have a card authorized by an NFC Enabler, most devices can make ordinary NFC transactions. RONS enables mobile transactions to be performed using NFC devices without dependencies. Although, in [26], the researcher studied and reviewed 12 papers from 2008 to 2015. They suggested establishing online payment transactions between NFC-enabled devices to be more secure. While considering the limited resources of NFC, the suggested protocol adds a new security surface designated Management Authentication Server (MAS). Furthermore, the findings demonstrate the protocol's resistance to various assaults. Ultimately, the protocol has several advantages, including scalability, simplicity, efficiency, and minimal computer processing administrative expenses. Thus, in [27], The GSM mobile jammer was designed and installed effectively. From a distance of 1.5m, the built detector circuit could identify the signal strength of an active mobile phone. The gadget detects the signal strength of an active phone and stops it from ringing by using both GSM 900 and GSM 1800 frequencies. The desired frequency for making noise during the jamming operation was obtained. Through [28], authors, in light of the ever-growing need for high-speed data, the overall number of subscriptions and connected devices will likely explode; it is anticipated that billions of devices will have been linked to the Internet by 2020, a 1000-fold increase. As a result, it is necessary to create a next-generation cellular technology community capable of fostering the emergence of billions of devices in an affordable and practical approach. The technique for accomplishing this is through energy efficiency. In addition [12], they studied and reviewed 16 papers from 2008 to 2016. This study provides a novel approach to improving the security of NFC payments by resolving the weaknesses in the EMV standard. The proposed protocol extends the EMV protocol with a security layer to secure the confidentiality of transmitted financial data and mutual authentication across the many actors participating in NFC payment transactions. The protocol successfully defends against malicious network attacks such as identity and replaying, session key protection, and brute force, especially man-in-the-middle. Subsequently, the protocol has several advantages: scalability, simplicity, cost-effectiveness, and minimal computer processing overheads. Lastly, in [10], the researchers studied 18 papers from 2012 to 2015. This study focused on security issues in MP. They represent a process of the MP model and introduce SMP. Also, they desired security services through SMP. However, to mitigate mobile payment risks, users and service providers must implement security measures to preserve data security and safeguard against data breaches.

Table 1: Past Studies.

Ref.	***Year***	***Description***
[18]	2023	The obstacles associated with digital payment systems were classified through five major categories: social, economic, technological, legal concerns, and public awareness. The major obstacles connected with growing digital payment methods were technical concerns such as privacy and security.
[21]	2022	In this project, they want to use NFC based on a safe protocol for mobile transactions. Furthermore, they employ a defense-in-depth strategy involving three tiers of mitigation: hardware, application, and communication.
[1]	2021	They explore several MPS-related security methods. They also analyze encryption technologies and authentication mechanisms, including firewalls in SMP. This study proposes many ways to offer various security elements. The essential aspect, however, is to verify the CIA triad upon each payment, which must be performed with identification and encryption since the future of SMP depends on security futures.
[22]	2021	Since traditional systems and PIN functionality have compromised user data, the authors propose a biometric system to recognize the authorized user. Difficulties with MP plus security may be minimized by using biometric technology systems for all data protection and completing transactions regularly. The payment method will also be an immediate enhancement through the use and assistance in advancing technology.
[23]	2020	Researchers have compared the framework they suggested and each of the three current solutions, which employ RSA and DES to protect and anonymize debit/credit card data. Many customers prefer an e-commerce program due to its numerous benefits. Customers want this kind of safe platform since it meets all standards and is adequate.
[24]	2020	This study discussed the MP security technology framework. Moreover, they identify and introduce secure technology, which includes hardware and software. Thus, they consider and examine the security concerns that they have faced, summarize unresolved difficulties, and offer future growth paths.
[25]	2019	Their technique can be applied to enterprises that utilize NFC-based transactions, such as secure entry to physical venues, mobile healthcare and banking apps, and mobile identity/access control choices. They want to employ RONFC for a range of mobile transactions shortly.
[27]	2019	The following piece will discuss current improvements in energy-efficient technology for sustained network deployment, which corresponds to conceptual 5G mobile technology from the standpoint of technology and deployment.
[26]	2018	The proposed protocol provides security for safe NFC communications between NFC-enabled devices and retailers (POS). The protocol effectively avoids malicious network attacks like impersonation and replaying, session key security breaches, brute force attacks, and man-in-the-middle attacks.
[28]	2018	This work aims to create a pocket-sized Global System for Mobile Communications (GSM) jammer device that transmits signals on the same frequency as the GSM system to prevent handheld devices from receiving and transmitting signals to the base station.
[12]	2017	This study proposes an efficient strategy for improving the security of NFC payments by addressing EMV protocol flaws. The suggested framework offers a security layer to the EMV protocol to protect the confidentiality of transmitted financial data and mutual authentication among the players in NFC payment transactions.
[10]	2016	They depict an MP processing paradigm and describe many types of MP systems. Furthermore, they highlight the security services sought in MP systems and the present security measures. Where they discover and analyze three more security concerns.

4. Threats and Attacks on Mobile Payment

Cybercriminals are targeting mobile payment systems. Several dangers and assaults have been discovered on mobile devices. These threats and assaults may also be directed at an SMP. Sharing an SMP could compromise the user's privacy and result in financial loss [10]. Contains in-depth analyses of mobile device dangers and assaults. This section summarizes the dangers and attacks that significantly influence MP security. The technology sector has used MP to allow clients to fully understand the positive aspects of these applications and transactions. Many consumers have been hesitant to embrace MP due to security concerns. The following items represent threats and assaults on MP issues that impact potential users, as depicted in Figure 5.

4.1 Mobile Wallets

4.1 SSL/STL Vulnerabilities

Several SMPs use SSL/TLS to protect data sent over the Internet. However, SSL/TLS and its use may contain weaknesses that malicious users could exploit to undermine security. SSL/TLS is also vulnerable to man-in-the-middle (MITM) attacks. In the SSL/TLS MITM attack, a rogue user sits between a client computer and an SSL/TLS server. All network communication between the client and the server side, which must be secured to prevent network sniffing, is exposed to the attacker in plain text. Sensitive information is at risk, particularly a username/password and credit card number. The attacker can steal money from compromised account holders or use these to commit fraud [10].

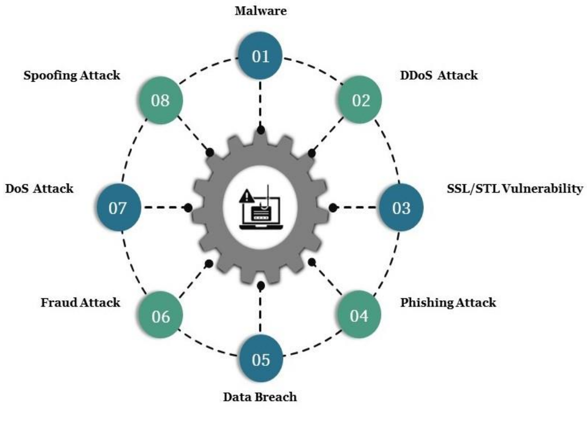

Fig. 5. Attacks Within MP.

4.2 Mobile Malware

Malware assaults are increasingly moving from conventional systems to online financial systems. Attackers have developed Malware targeting SMP, and the amount and varieties of Malware targeted SMP are expected to increase [32]. We will discuss the many forms of Malware that might harm MPS. It also displays several types of malware attacks that might occur in MP.

Keylogger: A keylogger is a malicious program that records anything someone puts on a computer. It may be used to steal a user's credentials (for example, their Internet banking information) and additional confidential data from a company.

Spyware: Spyware is software that captures sensitive data via a system (such as a smartphone). The collected data might be used in many ways, including marketing email addresses via cybercriminals.

Worm: A worm is a software that copies itself while destroying system files and information. It can spread over computer networks by exploiting holes in operating systems.

Virus: A virus is an infectious software that attaches itself to a separate piece of computer software and then rapidly replicates once the software executes.

Trojan: Trojan malware is meant to access someone's financial information and take control of the system's resources. An Android-infecting trojan program can utilize a connected mobile device to launch additional network assaults.

Rootkit: A rootkit is a type of Malware that hides either its own or a different initiative's presence (such as installing spyware on a smartphone) by leveraging operating system features that involve programming interfaces for applications and function redirection.

Hijacker: A hijacker, frequently called a computer hijacker, is a malicious application that primarily affects the online browser. It redirects normal search traffic and presents the results that its developers want users to observe.

Ransomware: This program disables or limits people from accessing their mobile device (such as a smartphone) by performing illegal activities such as hiding the system's display or locking the information stored by the user until a special payment (ransom) is paid.

4.3 Usage of Third-Party Applications

Third-party programs cannot be entirely trustworthy. Certain evil hackers and criminals created the programs.

4.4 Phishing and Pharming

These two types of dangers and attacks can occur when a person accesses public Wi-Fi or any other insecure network connection. Phishing occurs when a single attack evolves into several assaults, and the attackers have access to all data from all apps [33].

Table 2. Security Requirements for MP

4.5 Blockchain Vulnerability

There's an application for a functional system throughout blockchain and fog computing, according to [51]. The international financial system has been looking into how BCFC-based technologies involving financial assets like derivatives, instruments of fiat money, and equities might be used. Moreover, the employment of BC in the financial industry will result in cost savings in fields.

Furthermore, [31], there are threats and vulnerabilities throughout the blockchain that might let an attacker abuse the systems. The author's comparison provides a basic overview. Among the most frequent blockchain threats during [31] were DoS Attack, Sybil Attack, and Time-Jacking Assault.

Table 2: Security Requirements for MP

Security Requirements for MP	**Description**
Confidentiality	Individuals who can view financial data about various bank clients should have access to it.
Integrity	Under no circumstance must any unauthorized person (for instance, an attacker) modify and alter an institution's financial data.
Availability	Commercial data systems, including numerous banking servers, should be safeguarded from denial-of-service attacks.
Authentication	There are two authentication methods for online payment: **PIN code** authentication and **biometric identification**. The key difference between these two types is that the first type depends on a PIN code to be entered at the server located abroad, even though the latter is frequently biometrically confirmed locally. Both payment methods have their foundations in the hybrid's cryptosystem. [24] The process of authenticating an individual's (bank account holder's) identification is known as authentication. In this post, we will look at two types of multifactor authentication techniques: two-factor authentication and three-factor authentication. In two-factor authentication, someone utilizes two types of credentials, like a username and password, plus a smartphone or other mobile device (smart card). Once an individual joins with the server, both the smart card and the mobile device may preserve crucial data.[37]
Authorization	Authentication allows someone to perform a certain function. It prohibits mobile banking users from accessing information stored on banking servers to which they are entitled, for illustration, depending on their declared status in the system.
Physical theft of a device	Smart cards and mobile devices (smartphones) are critical information for secure and successful authentication. During stealing those devices, a range of attacks, such as authorized insider and offline/online password guessing attacks, can be carried out. [37]
Nonrepudiation	Nonrepudiation denotes that it is impossible to challenge the authenticity of the client's signature on a document or message the user sends.
Access Control	Access controls are a type of security constraint that restricts unauthorized activity access. Malicious conduct may be associated with the use of online and intranet resources. It also involves barriers, digital signatures, encryption, and various automated processes.

4.6 Data Breach

The following points constitute one of the most common and uncomfortable situations for new and unqualified clients. Customers' confidence may be harmed or destroyed as a consequence.

4.7 Fraud

MP is subject to fraud for older people since payment linkages may be made for receiving and transferring money. Although the link appears to have been used to receive money, the amount debited through the account is fake. These are possible in applications that use a client-to-customer model.

4.8 DoS Attack

This is an assault launched or directed by an electronic payments company that impacts MP authorization.

4.9 Distributed Denial of Service (DDoS)

A DDoS assault employs machines distributed throughout the Internet to consume resources. DDoS attacks are intended to achieve exactly what the term implies [34].

4.10 Spoofing Attacks

Attacks grow easier and more vulnerable when people are not alert when accessing the World Wide Web (the Internet) in public places, such as cross-site script attacks (XSS) [35].

5. Security Challenges on Mobile Payment

Certain security policies are essential to creating a secure environment during MP. We must be secure and free from danger in MP to gain user trust in all transactions. Thus, this section will review and discuss the requirements for MP, security solutions for MP threats and attacks, and limitations for secure MP.

5.1 Security Requirement for MP

Hardware makers, OS companies, platforms for payment vendors, and financial institutions can all supply these MP services [36]. Here, we will list the security requirements of MP to be secure and safe using MP. See Table 2, which represents a security requirement. There are several methods for ensuring the security of MP and applications.

5.2 Security Challenges

Several security protocols have been established to protect MP's safety. In contrast, MP poses security issues, including malware detection, multifactor authentication, data breach mitigation measures, and fraud detection and prevention.

5.2.1 Malware

Malware is a significant threat to MP security. Many safeguards have been put in place to detect and prevent malware propagation. Conversely, malware is still finding ways to increase its presence on mobile devices. The identification of mobile viruses is a tough task. There are now mobile forensics techniques, static evaluation, and dynamic examination, along with additional malware detection methods accessible. Considering this, none of these methods can identify Malware via mobile devices. An effective approach for identifying Malware is desired [38].

5.2.2 Multifactor Authentication

Two-factor authentication (2FA) uses two unique factors to access a platform. Two-factor authentication offers another layer of protection to electronic payments, making them safer and more private. [39] When a user signs up for a new mobile device, SMP may employ multifactor authentication to prevent fraud. Users must provide an authentication code received via a different method, such as email. Mobile devices whereas they could be lost or stolen. Malicious people with access to the email account may attempt to forge the multifactor authentication method.

The two-factor authentication approach has the potential to improve payment system security greatly. In addition to using passwords, users can employ effective methods such as biometrics and digital certificate verification to render it more difficult for bad actors to fraudulently exploit information. The verification code methodology is among the most commonly employed methods of implementing two-factor authentication. However, due to the basic leakage inherent simplicity underlying the verification process, vulnerabilities still need to be optimized.[40]

5.2.3 Data Breach

The following situation represents one of the most common and uncomfortable situations for new and unskilled clients. Customers' trust may be harmed or destroyed as a consequence of this. Data will probably be leaked. A data breach exposes private information such as cell phone values, credit card accounts, and transaction history. Users' privacy is jeopardized. It has the potential to lead to identity theft. [14,38]

5.2.4 Attacks Against Privacy

Individuals' ability to feel immunity to intrusion and breaches by other users is described as privacy. Challenged PINs used to obtain unauthorized knowledge of clients' financial assets and sensitive data utilized in unlawful activities are examples of privacy risks in MP.[29]

5.2.5 Attacks Against Integrity

The integrity of sensitive data is jeopardized when data about users is received and altered in the MMS. Insider attacks, salami attacks, and MITM attacks are the three categories. An intruder carries out an MITM attack by monitoring communications among various agents, especially customers within the MP app network. A hacker stands amid the MP client and MMS and pretends to interact with them in MITM and replay attacks [41].

5.2.6 Attacks Against Authentication

The authentication attack is a crime committed, while the MP authentication system is abused using a brute force attack on the PIN. Trojan horse attacks, phishing attacks, social engineering attacks, spoofing attacks, masquerade attacks, replay attacks, and impersonation attacks are a few instances of this assault [30].

5.2.7 Attacks Against Confidentiality

Monitoring the lines of communication between the application server and MP users to get information, such as user PINs, which may be employed for impersonation or unlawful transactions, is an instance of a confidentiality attack. These attacks are classified into four types: estimating assaults, brute force attacks, eavesdropping attacks, and should surfing attacks. Eavesdropping attacks include attackers listening in on communication channels invisibly via network communication security weaknesses. Such attacks are regularly launched against plain text data transport.

5.3 Security solutions for MP threats and attacks

An MP approach is a method that handles payments using Internet access and mobile devices [42]. Various security measures must be implemented to limit potential risks to MP. We will list a security solution for threats and attacks faced by MP.

5.3.1 Awareness

To enhance their knowledge, we must create awareness campaigns to educate MP consumers, systems, and bank employees about the hazards of Malware, phishing, and malicious file downloads.

5.3.2 Malicious Email Attachments

MP consumers should be careful because opening, downloading, or clicking on a file received as an attachment to an email may contain Malware.

5.3.3 Operating System Updates

Updating software is one of the many critical features of modern computing devices.

5.3.4 Protect Desktops

MP customers should install anti-virus programs on desktop computers.

5.3.5 Using Robust Authentication Schemes

A secure authentication mechanism is essential to protect the MP system. The suggested 3-digit security code solution is a third-step verification following the frequently employed two-step SMS code verification method, akin to an additional brief payment password [43].

5.4 Limitations for Security Solutions

Even with understanding and prudence, mobile banking security solutions have limits.

- Several organizations, including banks, provide security Awareness schemes for online and mobile banking consumers. Nevertheless, there is a need to implement security awareness initiatives in offline and online formats more regularly to ensure consumers are more informed of mobile banking risks.
- Multiple attacks may be launched using a mobile device's credit or debit card information. We must develop a secure authentication method even when submitted through an attacker's mobile phone via smart card attacks.
- Unknown abnormalities like zero-day attacks may impact the implemented security measures. As a result, the infrastructure for mobile banking should be unaffected.

6. Results Section

The following section will demonstrate our proposed authentication technique to validate the transaction process. We will start with a generic verification method, followed by a multifactor authentication process, followed by what results are achieved.

6.1 MP verification process

The verification technique entails collecting customer data, including biodata, fingerprints, and passwords, and then temporarily saving it in a mobile payment database. Every information the user gives is updated and recorded in a database, and a confirmation message is sent to the users via their phone numbers and emails recorded in the database for completed MP transactions or procedures. If the password is wrong and the face or touch ID does not identify the person, the operation will be aborted, and the user will be given three chances. The user is warned and encouraged to try again after three unsuccessful attempts. Figure 6 depicts the informational flow diagram associated with the MP verification procedure.

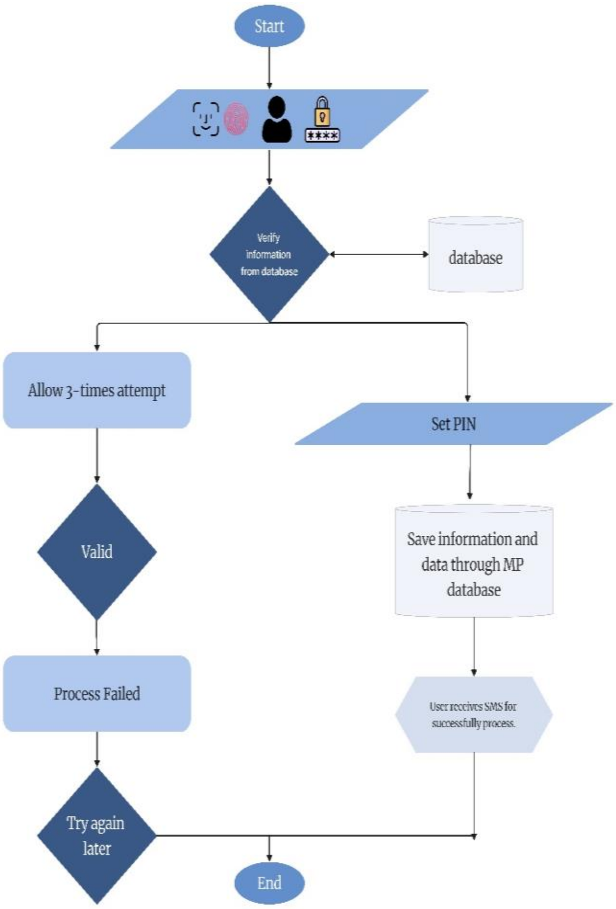
Start
****
Verify information from database
database
Allow 3-times attempt
Set PIN
Valid
Save information and data through MP database
Process Failed
User receives SMS for successfully process.
Try again later
End

Fig.6. MP verification workflow.

6.2 MP Authentication Approach

This is shown in Figure 7, which illustrates the authentication procedure required to secure and safe Internet transactions. Table 3 shows Algorithm 1.

Table 3. Algorithm 1

Algorithm 1	
Step 1	*Select the money needed to transfer.*
Step 2	*Fill in all information about the transaction,*
Step 3	*Choose an authenticating technique.*
Step 4	*Get OTP and send code via phone or email to authenticate before completion.*
Step 5	*Authenticate the process using passwords and biometrics.*
Step 6	*After the authentication is completed and the process is authenticated, we will send the user a message via phone that the process is completed.*
Step 7	*If the user doesn't authenticate the process, the process will end automatically.*
Output: *Process is authenticated and complete.*	

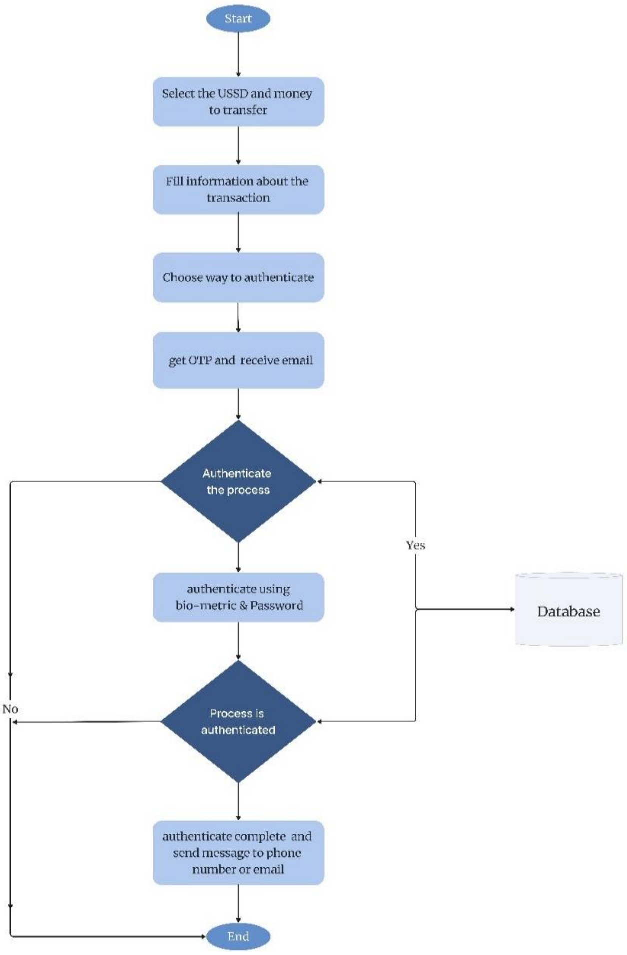
Start
Select the USSD and money to transfer
Fill information about the transaction
Choose way to authenticate
get OTP and receive email
Authenticate the process
Yes
authenticate using bio-metric & Password
Database
No
Process is authenticated
authenticate complete and send message to phone number or email
End

Fig.7. MP authentication workflow.

6.3 Ref. Results

Subsequently, this sub-section will present the findings of our investigation, beginning with a quick review of the number of references cited in our study. Figure 8 provides a concise overview of the references evaluated in this study.

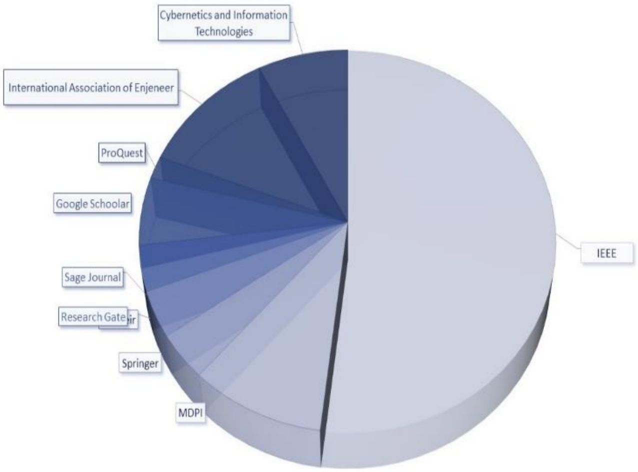

Fig.8. Summary of reviewed research studies.

We also worked and cited sources from 2016 to 2023. Table 4 shows a detailed breakdown of the sources—tables 1 and 5 show previous research relevant to our inquiry.

Table 4. Summary of Ref.

Ref	Amount of Ref.
IEEE	26
Elsevier	2
ProQuest	1
Springer	2
Google Scholar	2
MDPI	5
Research Gate	1
Sage Journal	1
International Association of Engineer	6
Journal of Physical Conference Series	1
Cybernetics and Information Technologies	4

7. Discussion Section

Due to the additional security mechanisms incorporated in the mobile app, frequent credit card payments are possible. When analyzing a payment system, several factors must be examined, which include authentication, encryption, and fraud detection. Authentication is essential to ensure that only those with permission can access the payment function. A strong and multifactor authentication technique, which might include

Fingerprint, or face recognition, should be used in a system. Encryption, however, ensures that payment information data, such as credit card numbers and account information, are securely stored and sent over the network. A good payment system must have risk management capabilities to identify and avoid suspicious activity, particularly fraud detection and prevention. [44,45] No standardized mobile payment schemes exist in many world regions. To provide payment dependability, both the trade environment and the transaction object should be dependable. The preservation of the anonymity of transaction information is referred to as data confidentiality. Furthermore, the transaction must be undeniable, implying that the participants must be irrefutable, although data integrity refers to avoiding harmful alterations throughout the transmission process [1]. Table 5 lists the benefits and drawbacks of using MP. Besides, Table 6 summarizes our work. Thus, the table represents the challenges, approaches, strengths, weaknesses, and proposed solutions for the previous studies, all related to MP. This table will specify the security challenges that faced MP.

Table 5. Benefits & Drawbacks of using MP.

Benefits	Drawbacks
1-Purchasers' expenses will be managed since they constantly check their virtual Wallet for payment history. [8] ***2- Ease of use:*** Clients may pay for items on a web store at any time and from any location. They want a gadget that can connect to the Internet. ***3- Contactless transactions:*** There is no requirement to be physically present to conduct any transaction. The quantity of money that may be sent through a single user's accounts to the receiver's accounts is limited, even though each transaction/exchange of cash may be done online. **4- *Privacy and Security:*** Most MP networks are protected by servers containing complete information and payment data. ***5- Availability 24*7:*** This constitutes one of the greatest advantages since transactions may be conducted at any time, from any location, and across any distance. **6- Safe and secure to use Wallet.** Thus, no costs are involved.	***1- Security concerns:*** Several security vulnerabilities involve contactless payment capabilities, whether wallets or MP. Our servers, clients, and wireless networks are all involved in all transactions. A security weakness on a single component of the system, alternately, the attacker can damage the entire system. ***2- Dependency:*** Clients fully rely on computer systems and network service providers. If there is an issue within the system or the web server, the client may be unable to complete the payment and must wait until the issue is rectified. ***3- Concerns about devices:*** Chip and mobile manufacturing companies constantly develop new features, forcing customers and network service providers to work together to upgrade and safeguard the system. ***4- Knowledge Enhanced:*** Users should be informed of the application, its capabilities, and the methods for completing the hassle-free payment. Consumers should be appropriately educated or instructed to execute payments without difficulty.

Table 6. Comparison Table.

Ref	Year	Challenges	Approach	Solutions	Strength/ Weakness
[48]	2023	Employ a switch non-scaling architecture to develop PTS of multiple integrator systems.	Depending on what the authors select, an appropriate switching mechanism is delivered via the given control system to assure the prescribed time consistency of the CLS origin.	The underlying PTS double integrator system successfully solves the computationally unique issue, resulting in a simpler controller.	--------------------
[2]	2023	Addressed security concerns resulting from the growing rise in mobile devices.	They made use of a digital wallet. The app generates a payment token with a range of data that could be	They suggested that architecture includes a methodology for securing numerous parts of an MP. The suggested	The strength of existing MP systems was meant to conform with old payment structures, limiting cellphones' full capabilities,

			utilized to perform authentication.	architecture helps to assure transaction validity, reduce identity theft, and improve user ease.	especially their security features.
[46]	202 2	Path planning has considered optimization problems in recent years, which is important in mobile robot navigation.	The current investigation focuses on an algorithm constructed using GA and IACO that works within a static environment to tackle GPP problems.	They used GA-IACO to create a hybrid algorithm for rapid path selection and changing crossover operators, lowering the chance of falling.	The findings of this investigation proved that the robot can safely travel from one spot to another.
[47]	202 2	Forward Station Mobile Communication System (FRMCS) 5G technology should meet the growing continuously seamless connection requirements associated with millimeter wave and huge Numerous Input Multiple Output (MIMO) capabilities.	This investigation intends to develop an ideal 26 Ghz outdoor antenna micro-strip design for the next-generation Railway Mobile Communication System (FRMCS) in a 5G communications system. The micro-strip feeding approach has been employed to feed the prescribed structure of a 2 × 2 antenna patch with 112 radiations. The simulation of the built design is carried out using the CST Microwave Studio tool.	The return-on-investment loss value of -11.113 dB, the VSWR value of 1.7712, and the significant gain of the antenna of 14.89 dBi all yield satisfactory outcomes.	The achieved state of the ideal layout has significance for achieving the criterion of smooth connectivity for FRMCS deployment. The simulation's powerful gains from the antenna are enough to fulfill the difficult requirements of overcoming air attenuations of greater mobility and frequencies.
[22]	202 1	Because of the rising usage of mobile phones and tablets, security, and hazards have become a concern for the many actors in the MP system. All stakeholders collaborate to ensure that the system is safe for risk-free payments. On the other hand, virus attacks and malicious users are considered overheads in MP networking both at the client and server stages.	Considering that traditional systems and PIN functionality have compromised user data, the authors propose a biometric system to recognize the authorized user uniquely.	Researchers proposed security procedures and preventions implemented by stakeholders to ensure the payment network's secure operation.	--------------------
[30[	202 1	The various elements include security issues, MPS core qualities, and customer and communication entity responsibilities in MP.	M-Payment process	They propose many strategies to give various levels of protection. However, keeping the CIA trinity in mind, Since the future of MP is based on its security features, each payment should be made using authentication and encryption.	The research is robust and includes concepts and techniques for security, but it only provides findings based on their actual experiences and activities.

[21]	2021	Attacks and threats on MP.	Developers use the Kotlin programming language in Android Studio to create their protocol, which includes several applications and POS.	They suggested that protocol assures all security features based on NFC and the energy, communication, and computing costs.	The protection-in-depth method is divided into three levels: hardware defense, application defense, and communication defense. All known attacks, including multiprotocol assaults, are defeated by the proposed protocol. Their suggested protocol consumes less energy, has lower transmission costs, and has a lower computing cost than previous works.
[49]	2020	The present study investigates the challenge of fixed-time stabilizing control for a wheeled mobile robot with a space limitation.	The nonlinear mapping method changes the limited system towards an alternative unlimited one. Following that, by combining a power integrator approach and switching control tactics, a conditional feedback controller is successfully built to ensure that the closed-loop system's states can be controlled to zero in a given set period without violating the constraint.	When combined with a new switching control technique, the newly developed controller may ensure that the closed-loop system conditions are regulated to zero for a particular fixed duration while ensuring the constraint is not violated.	The simulation findings are provided to validate the efficacy of the suggested control mechanism.
[32]	2019	Threats on MP, such as Malware with different types and classification	They discussed various requirements to be secured.	They proposed updating your devices and being aware of protection through the MP.	--------------------
[10]	2016	MP faced several security dangers and hurdles. Malware detection, multiple-factor authentication, and data breach protection are all issues.	Experts highlighted security issues like Malware, SSL/TLS flaws, and data leaks.	To mitigate mobile payment risks, customers and service providers must implement security measures to preserve the privacy of information and prevent data breaches.	--------------------
[50]	2023	Optimize cryptocurrencies utilizing the XGBoost technology.	Practical swarm optimization (PSO) approach.	The PSO Algorithm, when utilized with pre-processed trade information, has a greater capacity to select the most effective global optimum solutions in the continuous search space.	The PSO Algorithm offers a stronger capacity to choose the best global optimal solution within an ongoing search space when pre-processed trading knowledge is used.

8. Conclusions & Future Work

The convenience of mobile payments (MP) has led to widespread adoption across various domains. In addition to the benefits of MP, Near Field Communication (NFC) technology offers the advantage of integrating multiple services into a single mobile device. This research aims to analyze different MP models and their underlying procedures comprehensively. Moreover, we delve into the security challenges, threats, and attacks that MP encounters. Among the significant threats MP faces, Malware stands out as one of the most hazardous. To safeguard their mobile devices, users must enhance their security knowledge and take proactive measures to prevent malware infections. Mitigating the risks associated with Malware is crucial in ensuring the secure operation of MP systems. In addition to Malware, other significant security concerns within the MP landscape revolve around SSL/TLS flaws and data breaches. Vulnerabilities in the secure socket layer (SSL) and transport layer security (TLS) protocols pose potential risks to the confidentiality and integrity of MP transactions. Therefore, addressing and resolving these flaws are paramount to maintaining robust security in MP ecosystems. Furthermore, data breaches can have severe consequences, including unauthorized access to sensitive user information and financial losses. Implementing stringent data protection measures is imperative to prevent such breaches and protect the privacy of MP users. By thoroughly examining these security challenges, threats, and vulnerabilities, this research aims to provide valuable insights into fortifying the security of MP systems. It emphasizes the need for continuous advancements in security practices, user awareness, and technology to ensure the resilience and integrity of mobile payment environments.

References

[1] V. Njebiu, M. Kimwele and R. Rimiru, "Secure Contactless Mobile Payment System," 2021 IEEE Latin-American Conference on Communications (LATINCOM), Santo Domingo, Dominican Republic, 2021, pp. 1-6, doi: 10.1109/LATINCOM53176.2021.9647831.

[2] Alamleh, H., AlQahtani, A. A. S., & Smadi, B. A. (2023). Secure mobile payment architecture enabling multifactor authentication. Ithaca: Cornell University Library, arXiv.org. Retrieved from https://www.proquest.com/working-papers/secure-mobile-payment-architecture-enabling-multi/docview/2803674803/se-2.

[3] M. Bosamia, "Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its Possible Security Measures," in International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017), CHARUSAT, Changa, India, 2017.

[4] Al-Haija, Q.A.; Alsulami, A.A. High Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. Electronics 2021, 10, 2113. https://doi.org/10.3390/electronics10172113.

[5] M. Al-Tamimi and A. Al-Haj, "Online security protocol for NFC mobile payment applications," 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 2017, pp. 827-832, doi: 10.1109/ICITECH.2017.8079954.

[6] Al-Haija QA, Alnabhan M, Saleh E, Al-Omari M. Applications of blockchain technology for improving security in the Internet of things (IoT). InBlockchain Technology Solutions for the Security of Iot-Based Healthcare Systems 2023 Jan 1 (pp. 199-221). Academic Press.

[7] A. Badawi and Q. A. Al-Haija, "Detection of money laundering in bitcoin transactions," 4th Smart Cities Symposium (SCS 2021), Online Conference, Bahrain, 2021, pp. 458-464, doi: 10.1049/icp.2022.0387.

[8] S. Saxena, S. Vyas, B. S. Kumar, and S. Gupta, "Survey on online electronic payments security," in Proc. Amity Int. Conf. Artif. Intell. (AICAI), Feb. 2019, pp. 751–756.

[9] A. Brohi et al., "Near field communication enabled payment system adoption: A proposed framework," 2017 IEEE 3rd International Conference on Engineering Technologies and Social Sciences (ICETSS), Bangkok, Thailand, 2017, pp. 1-5, doi: 10.1109/ICETSS.2017.8324199.

[10] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 2016, pp. 1-5, doi: 10.1109/MOBISECSERV.2016.7440226.

[11] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, "Secure Authentication Protocol for Mobile Payment," in Tsinghua Science and Technology, vol. 23, no. 5, pp. 610-620, Oct. 2018, doi: 10.26599/TST.2018.9010031.

[12] Ghosh, Shirsha & Majumder, Alak & Goswami, Joyeeta & Kumar, Abhishek & Mohanty, Saraju & Bhattacharyya, Bidyut. (2017). Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment. IEEE Consumer Electronics Magazine. 6. 82-93. 10.1109/MCE.2016.2614522.

[13] M. Obaid, Z. Bayram, and M. Saleh, "Instant Secure Mobile Payment Scheme," in IEEE Access, vol. 7, pp. 55669-55678, 2019, doi 10.1109/ACCESS.2019.2913430.

[14] G. Ali, M. A. Dida, and A. E. Sam, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures," Future Internet, vol. 12, no. 10, p. 160, Sep. 2020.

[15] K. Albulayhi and Q. A. Al-Haija, "Early-stage Malware and Ransomware Forecasting in the Short-Term Future Using Regression-based Neural Network Technique," 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, 2022, pp. 735-742, doi: 10.1109/CICN56167.2022.10008270.

[16] Q. A. Al-Haija, "Time-Series Analysis of Cryptocurrency Price: Bitcoin as a Case Study," 2022 International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT),

Jember, Indonesia, 2022, pp. 49-53, doi: 10.1109/ICEECIT55908.2022.10030536.

[17] J. Sun and N. Zhang, "The mobile payment based on public-key security technology," J. Phys., Conf. Ser., vol. 1187, no. 5, Apr. 2019, Art. no. 052010.

[18] Khando, K., Islam, M. S., & Gao, S. (2023). The emerging technologies of digital payments and associated challenges: A systematic literature review. Future Internet, 15(1), 21. Doi https://doi.org/10.3390/fi15010021.

[19] Ketipov,R.,Angelova,V.,Doukovska,L. & Schnalle,R.(2023).Predicting User Behavior in e-Commerce Using Machine Learning. Cybernetics and Information Technologies,23(3) 89-101. https://doi.org/10.2478/cait-2023-0026.

[20] Popchev I, Ketipov R, Angelova V. Risk averseness and emotional stability in e-commerce. Cybernetics and Information Technologies. 2021 Sep 1;21(3):73-84.

[21] S. S. Ahamad, "A Novel NFC-Based Secure Protocol for Merchant Transactions," in IEEE Access, vol. 10, pp. 1905-1920, 2022, doi: 10.1109/ACCESS.2021.3139065.

[22] Galhotra, A. Jatain, S. B. Bajaj and V. Jaglan, "Mobile Payments: Assessing the Threats, Challenges and Security Measures," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2021, pp. 997-1004, doi: 10.1109/ICECA52323.2021.9676092.

[23] Hassan, M. A., Shukur, Z., Mohammad, K. H., & Al-Khaleefa, A. (2020). A review on electronic payments security. Symmetry, 12(8), 1344. Doi https://doi.org/10.3390/sym12081344.

[24] W. Liu, X. Wang, and W. Peng, "State of the Art: Secure Mobile Payment," in IEEE Access, vol. 8, pp. 13898-13914, 2020, doi: 10.1109/ACCESS.2019.2963480.

[25] Turk, P. Angin and A. Cosar, "RONFC: A Novel Enabler-Independent NFC Protocol for Mobile Transactions," in IEEE Access, vol. 7, pp. 95327-95340, 2019, doi: 10.1109/ACCESS.2019.2929011.

A.Al-Haj and M. A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," 2018 4th International Conference on Information Management (ICIM), Oxford, UK, 2018, pp. 184-187, doi: 10.1109/INFOMAN.2018.8392832.

[26] Nsikan Nkordeh, Akindele Ayoola, Opeoluwa Bankole, Oloyede Oludotun, Ekwenem Nwabueze, and Okpor Paul Chidi, "Green Computing: Towards Sustainable 5G Network Deployment," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2019, 22-24 October, 2019, San Francisco, USA, pp140-143.

[27] Albert Kofi Kwansah Ansah, "Design and Implementation of a GSM Mobile Detector and Jammer," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2018, 23-25 October 2018, San Francisco, USA, pp95-101.

[28] Abu Al-Haija Q, Mohamed O, Abu Elhaija W. Predicting global energy demand for the next decade: A time-series model using nonlinear autoregressive neural networks. Energy Exploration & Exploitation. 2023;0(0). doi:10.1177/01445987231181919.

[29] W. Ahmed et al., "Security in Next Generation Mobile Payments Systems: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 115932-115950, 2021, doi: 10.1109/ACCESS.2021.3105450.

[30] Qaqish E, Aranki A, Al-Haija QA, Qusef A. Security Comparison of Blockchain and Cloud-based Identity Management: Considering the Scalability Problem. In2023 International Conference on Inventive Computation Technologies (ICICT) 2023 Apr 26 (pp. 1078-1085). IEEE.

[31] M. Wazid, S. Zeadally, and A. K. Das, "Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions," in IEEE Consumer Electronics Magazine, vol. 8, no. 2, pp. 56-60, March 2019.

[32] Abu Al-Haija, Q., Al-Fayoumi, M. An intelligent identification and classification system for malicious uniform resource locators (URLs). Neural Comput & Applic (2023). https://doi.org/10.1007/s00521-023-08592-z.

[33] Droos A, Al-Haija QA, Alnabhan M. Lightweight detection system for low-rate DDoS attack on software-defined-IoT. In6th Smart Cities Symposium (SCS 2022) 2022 Dec 6 (Vol. 2022, pp. 157-162). IET.

[34] [35] Al-Haija QA. Cost-effective detection system of cross-site scripting attacks using a hybrid learning approach. Results in Engineering. 2023 Jun 27:101266.

[35] Kang, J. (2018). Mobile payment in fintech environment: Trends, security challenges, and services. Human-Centric Computing and Information Sciences, 8(1), 1-16. Doi https://doi.org/10.1186/s13673-018-0155-4.

[36] F. Altwairqi, M. A. AlZain, B. Soh, M. Masud, and J.

Al-Amri, "Four most famous cyber-attacks for financial gains," Int. J. Eng. Adv. Technol. vol. 9, pp. 2131–2139, Dec. 2019.

[37] A. Ortiz-Yepes, "A Review of Technical Approaches to Realizing Near-Field Communication Mobile Payments," in IEEE Security & Privacy, vol. 14, no. 4, pp. 54-62, July-Aug. 2016, doi: 10.1109/MSP.2016.75.

[38] Nagre and A. Sen, "Study Of Security Postures In Payment Gateways Using a Case Study Approach," 2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand, 2022, pp. 534-538, doi: 10.1109/DASA54658.2022.9765163.

[39] Chen, "Discussion on the Security Mechanism of Mobile Payment," 2021 7th Annual International Conference on Network and Information Systems for Computers (ICNISC), Guiyang, China, 2021, pp. 65-68, doi: 10.1109/ICNISC54316.2021.00020.

[40] Abu Al-Haija, Q.; Alsulami, A.A. Detection of Fake Replay Attack Signals on Remote Keyless Controlled Vehicles Using Pre-Trained Deep Neural Network. Electronics 2022, 11, 3376. https://doi.org/10.3390/electronics11203376

[41] Puneet Kaur, Amandeep Dhir, Naveen Singh, Ganesh Sahu, Mohammad Almotairi, An innovation resistance theory perspective on mobile payment solutions, Journal of Retailing and Consumer Services, Volume 55,2020,102059, ISSN 0969-6989, https://doi.org/10.1016/j.jretconser.2020.102059.

[42] R. Xu, "Security Enhancement for SMS Verification Code in Mobile Payment," 2022 11th International Conference of Information and Communication Technology (ICTech)), Wuhan, China, 2022, pp. 3-7, doi: 10.1109/ICTech55460.2022.00008.

[43] Alamleh, Hosam & Alqahtani, Ali & Al Smadi, Baker. (2023). Secure Mobile Payment Architecture Enabling Multifactor Authentication.

[44] Y. Madwanna, M. Khadse and B. R. Chandavarkar, "Security Issues of Unified Payments Interface and Challenges: Case Study," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 2021, pp. 150-154, doi: 10.1109/ICSCCC51823.2021.9478078.

[45] Hong Chen, "Path Planning of Mobile Robot Using Hybrid Algorithm Based on GA-IACO," Engineering Letters, vol. 30, no.2, pp582-589, 2022.

[46] Selvi Lukman, Yul Yunazwin Nazaruddin, Bo Ai, and Endra Joelianto, "The Optimal Design of 26 Ghz 5G-R Micro-strip MIMO Outdoor Antennas for Future Railway Mobile Communication System," Engineering Letters, vol. 30, no.4, pp1662-1668, 2022.

[47] Yuhang Cao, Yanling Shang, Wendian Zhang, Jiacai Huang, and Fangzheng Gao, "Prescribed-Time Stabilization of Double Integrator Systems with Application to Wheeled Mobile Robot," IAENG International Journal of Applied Mathematics, vol. 53, no.1, pp108-112, 2023.

[48] Yanling Shang, and Jiacai Huang, "Fixed-Time Stabilization of Spatial Constrained Wheeled Mobile Robot via Nonlinear Mapping," IAENG International Journal of Applied Mathematics, vol. 50, no.4, pp791-796, 2020. ‘

[49] Srivastava V, Dwivedi VK, Singh AK. Cryptocurrency Price Prediction Using Enhanced PSO with Extreme Gradient Boosting Algorithm. Cybernetics and Information Technologies. 2023 Jun 1;23(2):170-87.

[50] Alzoubi YI, Aljaafreh A. Blockchain-Fog Computing Integration Applications: A Systematic Review. Cybernetics and Information Technologies. 2023 Mar 1;23(1):3-7.

Appendix

Table 7. List of Abbreviations.

Abbreviation	**Description**
POS	Point of Sales.
USSD	Unstructured Supplementary Service Data.
NFC	Near Field Communication.
MNO	Mobile Network Operator.

Abbreviation	**Description**
SMS	Short Message Services.
BTS	Base Transceiver Station.
SMP	Secure Mobile Payment.
P2P	Peer to Peer.
MP	Mobile Payment.
OTP	One-Time Password.
PIN	Personal Identification Number.
TLS	Transport Layer Security.
EMV	Europay, Mastercard & Visa.
MITM	Man in the Middle attack.
DoS	Denial of Services.
RONFC	Read Only NFC.
PTS	Prescribed-Time Stabilization.
GPP	Global Path Planning.
USSD	Unstructured supplementary service data.