IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 4, 2021, accepted August 11, 2021, date of publication August 16, 2021, date of current version August 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3105450

Security in Next Generation Mobile Payment Systems: A Comprehensive Survey

WAQAS AHMED[1], AAMIR RASOOL[1], ABDUL REHMAN JAVED[1], (Member, IEEE), NEERAJ KUMAR[2,3], (Senior Member, IEEE), THIPPA REDDY GADEKALLU[4], ZUNERA JALIL[1], (Member, IEEE), AND NATALIA KRYVINSKA[5]

[1]Department of Cyber Security, Air University, Islamabad 44200, Pakistan
[2]Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala, Punjab 147004, India
[3]School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand 248007, India
[4]School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
[5]Faculty of Management, Comenius University in Bratislava, 82005 Bratislava, Slovakia

Corresponding authors: Abdul Rehman Javed (abdulrehman.cs@au.edu.pk) and Natalia Kryvinska (natalia.kryvinska@uniba.sk)

ABSTRACT Cash payment is still king in several markets, accounting for more than 90% of the payments in almost all the developing countries. The usage of mobile phones is pretty ordinary in this present era. Mobile phones have become an inseparable friend for many users, serving much more than just communication tools. Every subsequent person is heavily relying on them due to multifaceted usage and affordability. Every person wants to manage his/her daily transactions and related issues by using his/her mobile phone. With the rise and advancements of mobile-specific security, threats are evolving as well. In this paper, we provide a survey of various security models for mobile phones. We explore multiple proposed models of the mobile payment system (MPS), their technologies and comparisons, payment methods, different security mechanisms involved in MPS, and provide analysis of the encryption technologies, authentication methods, and firewall in MPS. We also identify current challenges and future directions of mobile phone security.

INDEX TERMS Mobile payment method, online system, transaction, mobile commerce, cyberattacks.

I. INTRODUCTION

Cash payment is still monarch in several markets, accounting for more than 90% of the payments in all almost all the developing countries [1]. Nowadays, the use of mobile devices by people has increased tremendously. A considerable number of people use mobile phones to perform day-to-day tasks [2]. These devices can be used for many tasks, such as making phone calls, web surfing, emailing, gaming, and many other tasks.

The current research in this area is focused on the usage of mobile phones to perform payment securely. However, mobile systems face several limitations [3]–[5] such as low storage and computation power, due to which they cannot perform heavy encryption operations. Different attacks are reported on mobile devices due to lack of security patches such as spoofing, phishing, malware, and sniffing attacks [6]–[9]. In order to effectively design the MPS, these attack scenarios must be considered for safety and security.

Information and communication technology (ICT) is being extensively used all around the world [10]. The traditional face-to-face interaction requirement for payment transactions is avoided, and remote communication is adopted. There is no need for direct contact between a payer and the payee that changes the business environment and leads towards using the Internet to do different transactions. This situation requires electronic money or digital bits; the system resembles traditional payment but uses internet infrastructure and digital data for money transfer. There are many advantages of using e-money, like the client's anonymity or the client's presence is not required during transactions. At the same time, it also has some disadvantages, like compromising of confidentiality, integrity, and availability (CIA) [11].

The vast development of mobile phone technology enables the growth of internet services. Internet brings the electronic transaction systems [12] to the mobile phones and also m-commerce [13] becomes an alternative for e-commerce.

The associate editor coordinating the review of this manuscript and approving it for publication was Yuan Gao.

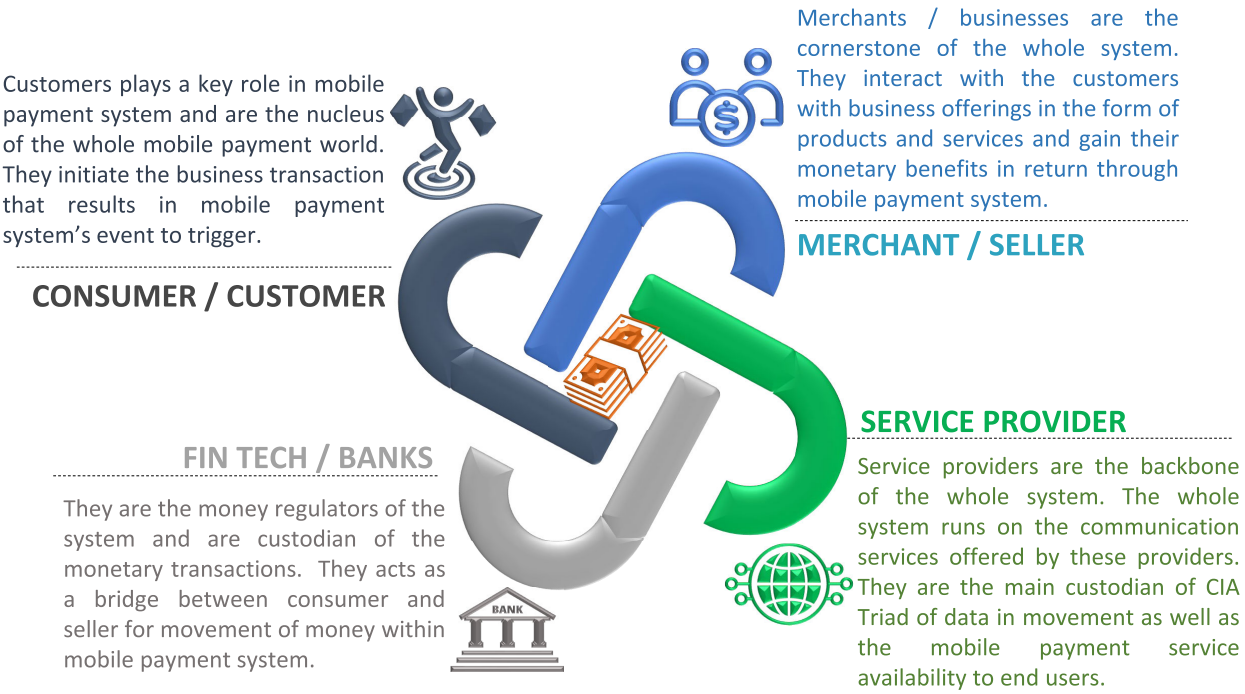


FIGURE 1. Major components of MPS.

As m-commerce is growing at a tremendous pace, it is getting much more attention than e-commerce nowadays. M-commerce has the same characteristics [14] as e-commerce with some extra advantages like Mobile Payment System (MPS), which allows clients to perform transactions in real-time by using mobile phones anywhere; all it needs is internet connectivity. Another advantage is that, unlike a PC, one can carry his/her mobile phone anywhere. Some other benefits are interoperability, speed, cost, and cross-border payments. Figure 2 shows a Mobile Management system.

A MPS should include authentication, access control, confidentiality, integrity, non-repudiation, and availability [15]. The authentication process includes two steps: verification of the user and verification of the origin. In authentication, two processes include verifying the user and the origin of the source of data. Access control can grant access to an authorized person to the payment system and block unauthorized personnel from accessing the payment system. The information must also remain hidden to avoid passive attacks against transaction data. Availability ensures that the payment system is accessible. Integrity avoids the modification of data and non-repudiation ensures that a specific user has transmitted the message.

Security is essential for MPS, and many security standards such as payment card industry data security standard (PCIDSS) [16], which was first released in 2004, are used to maintain the CIA triad. The people or merchants who use payment cards follow PCIDSS standards but security violations can still occur [6], [17]. When security violations occur, personal information and payment card information such as expiration date, ATM card number, security code, and transaction ID are at risk, leading to fraud or illegal usage of service. There are two methods of Mobile Payment Systems: account-based payment system and token-based payment system [18].

1) ACCOUNT BASED PAYMENT SYSTEM

In account-based transactions, we need cards or information cards like ATMs or credit cards. Using this process, the user's bank account charges the amount after getting the required details or confirmation of the user's transaction.

Risk Factor: If any misuse of a card or details is done or any forgery or identity theft is done, then it will affect this system.

2) TOKEN BASED PAYMENT SYSTEM

It is a new electronic payment method based on tokens instead of cash or credit cards. These tokens are generated by any bank, service provider, or telecom company. Moreover, it is used in the same way as cash is used. By using such tokens, users can pay to any company through mobile, and those tokens will be sent to that company which they can encash, or the provider will pay them for each token.

Risk Factor: These tokens will have no worth if the user has tokens in their account and the merchant does not accept those tokens.

A. MOTIVATION

Mobile phones' usage is highly elevated in the current era compared to their usage a decade before. The number of mobile phones is higher than the number of bank

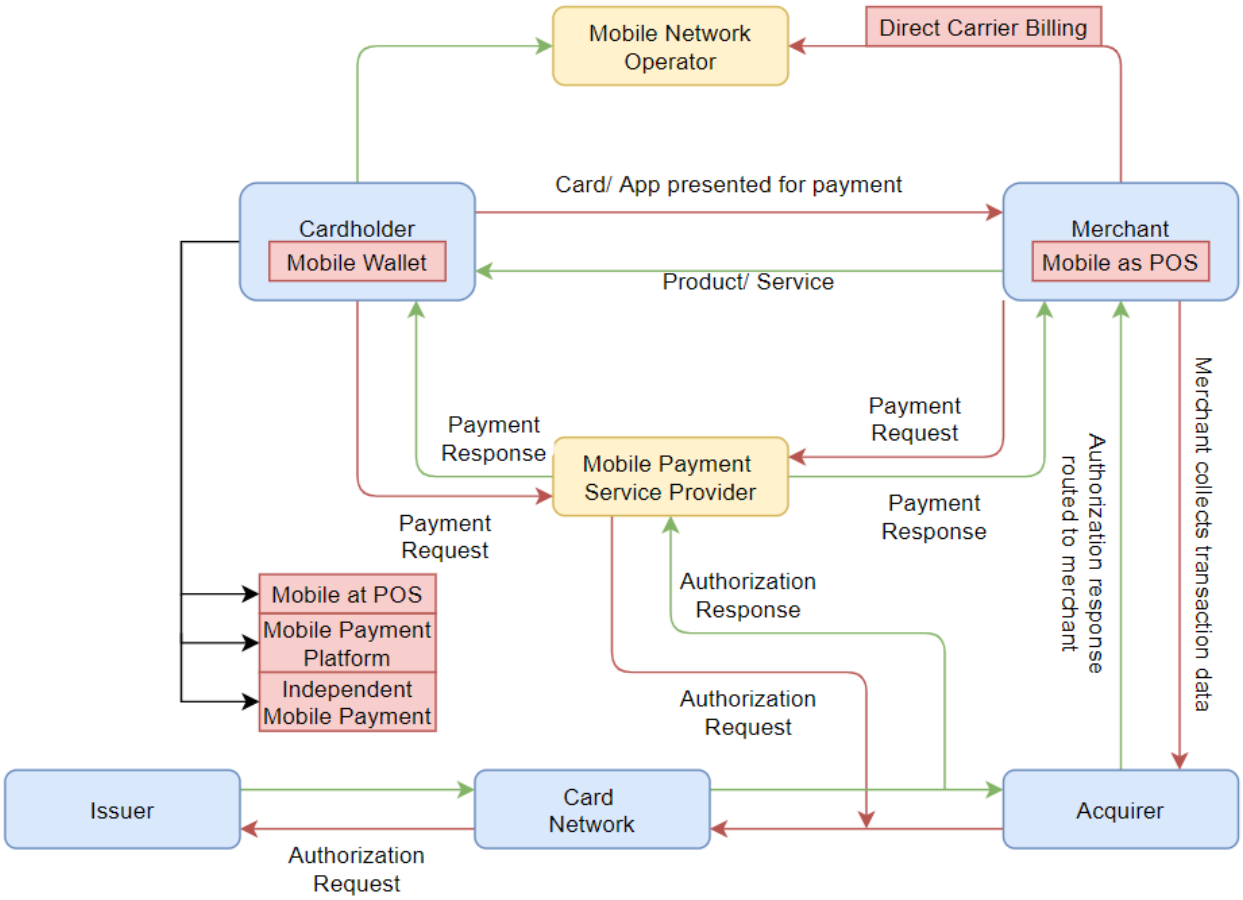


FIGURE 2. Mobile management system.

accounts that exist. Due to its high usage level, most business organizations, the entertainment industry, banks, the education sector, and almost all fields turn towards mobile phone adaptability. To benefit from this device, they launch their applications for the comfort of people. Almost all banks facilitate consumers with mobile phone applications. People use mobile phones for shopping, transferring money, and getting various services. The maximum use of mobile devices and versatility motivate us to focus on mobile payment systems (MPSs). Different models of payment systems have been proposed, but many limitations exist, such as security and privacy concerns. Figure 3 shows the increased usage of MPS in the United States from 2016 onwards and sheds light on the adoption rate and numbers of users (in millions) in a single glance.

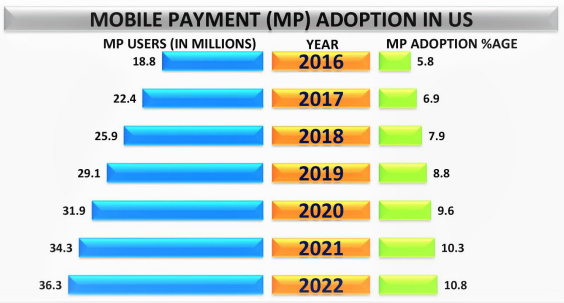


FIGURE 3. Proximity mobile payment adoption in the United States from 2016 onwards.

B. CONTRIBUTION

This review paper aims to present an in-depth analysis and survey of MPS. This paper makes the following contributions:

1) We present an overview and discuss different components of MPS. We present a review of the existing MPS structure and its limitations.
2) We discuss and analyze the two main methods of MPS, including account-based payment systems and token-based payment systems.
3) We provide detailed history, development, and deployment of MPS and discuss aspects of MPS, including socioeconomic conditions, cost efficiency, diffusion of mobile phones, convenience, new initiatives, heavy restrictions and regulations, limited collaboration, underdeveloped ecosystem, and security problems.

4) We discuss key attributes of MPS, and stakeholder and communication entities' roles in MPS form different aspects.
5) We demonstrate the security mechanisms involved in MPS. Provide analysis of the encryption technologies, authentication methods, and firewall in MPS.
6) We present authentication techniques (one way, two way, and multiple way authentication) in MPS and discuss the mentioned techniques' pros and cons.
7) Provide analysis of the various possible attacks on MPS, including attacks against user privacy, attacks on authentication techniques, attacks on user confidentiality data, attacks on the data integrity, and attacks against MPS services availability.
8) Next, we provide key challenges developers and researchers face in implementing and deploying MPS. In the end, we present different research directions related to MPS.

The rest of the paper is organized as follows: Section II-A discusses the history, development, and deployment of the mobile payment system; Section II-D discusses the generic architecture of the M-Payment system; Section VI presents technologies used in the M-Payment system and their comparison; Section VII provides a comparison of security aspects in different mobile payment models; and at the end, Section IX provides the current challenges, future direction followed by Section VIII which concludes the works.

II. RELATED WORK

Cash payment accounts for more than 90% of the payments in all almost all the developing countries [1]. Therefore, it is essential to realize the importance of MP acceptance. Different researchers have presented several research studies on MP after the first MP transaction performed in 1997 [19], [20]. Several studies on MP implementation have focused on the user side, considering the user's behavior on MP is significant to advance MP services to improve users acceptance intention [21].

The authors in [22] tried to respond to specific questions related to the security of online payment systems and present several ways to overcome different security threats associated with online payment systems. Similarly, the authors in [23] present different types of online payments such as credit card, e-wallet, debit card, net banking, smart card, mobile payment, and amazon pay. The authors also present some requirements for online payments such as integrity and authorization, out-band authorization, password authorization, signature authorization, confidentiality, and availability and reliability. Later, the authors in [24] proposed a new secure authentication protocol (SAP) for mobile payment. The authors used cryptography techniques for the authentication between server and client. The proposed technique provides security to user data account and provides privacy during the payment transaction.

This work reviews the literature work of MP in the following significant areas: mobile payment system (MPS): history, development, and deployment; factors limiting MP development; MPS key attributes; and MP stakeholders and entities. Table 2 presents the comparison of the existing survey papers on MP.

TABLE 1. List of abbreviations.

Abbreviation	Description
MPS	Mobile Payment System
ICT	Information and Communication Technology
CIA	Confidentiality, Integrity and Availability
MMS	Mobile Management System
PCI	Payment Card Industry
DSS	Data Security Standard
PTC	Pakistan Telecommunication
TAM	Technology Acceptance Model
EPS	Electronic Payment System
TE	Technology Evolution
CPT	Cart Present Transactions
SEM	Structural Equation Model
NFC	Near Field Communication
QR	Quick Response
SMS	Short Message Service
MB	Mobile Banking
MP	Mobile Payments
MW	Mobile Wallets
MC	Mobile Currency
MFS	Mobile Financial System
MNO	Mobile Network Operators
DS	Digital Signature
CA	Certificate Authority
RA	Register Authorities
SKE	Symmetric Key Encryption
PKE	Public-Key Encryption
PIN	Personal Identification Number
MFA	Multifactor Authentication
SFA	Single-Factor Authentication
2FA	Two-Factor Authentication
DDOS	Distributed Denial-of-Service Attack
DOS	Denial-of-Service Attack
OTP	One Time Password
USSD	Unstructured Supplementary Service Data
GSM	Global System for Mobile
RFID	Radio Frequency Identification
QRC	Quick Response Code
WAP	Wireless Application Protocol
U2F	Universal 2nd Factor
MAC	Message Authentication Code
SAP	Secure Authentication Protocol

A. MOBILE PAYMENT SYSTEM (MPS): HISTORY, DEVELOPMENT, AND DEPLOYMENT

MPS provides several payment facilities for different kinds of services, products, and bills through mobile phones by using wireless characteristics and other features and benefits of a communication system [35]. Mobile devices like smartphones, smart tablets are utilized in different payment scenarios such as purchasing online tickets, electronic materials, online electronic transactions, and transport fares such as paying bills and other invoices. It is also possible to purchase products physically through MPS, from the point-of-sale (PoS), ticketing machines, and vending machine stations. Besides that, most electronic payment systems and payment instruments nowadays have also been mobilized [36].

The field of MPS is relatively new, and little is known about it. Mobile phones are more than just a payment method. Instead, it is a method of initiating, processing, and confirming financial transactions. Mobile payments are not

TABLE 2. Research literature comparison.

Ref.	Proposed	Outcomes
[25]	To integrate choice-based conjoint (CBC) and system dynamics (SD), the author develops an empirical data-driven simulation methodology to analyze several competing diffusion dynamics mobile payment platforms.	To collect multi-attribute preference data, a choice-based conjoint analysis methodology is used on a different platform. To evaluate the effect of platform design strategies, an empirical user preference SD simulation model is developed with the help of an empirical user preference data model.
[26]	The author in this study aims to compare different factors that define consumers' acceptance for near field communication (NFC) and short message service (SMS) as examples of means for mobile payment of future payment systems.	From the most relevant literature review, a model is driven and used in this research that applies the perceived security (PS) and technology acceptance model (TAM). The results succeeded in this research work in determining the differences between the different factors that define the acceptance of the Mobile Payment Systems and the intention to use level of the users.
[22]	The author discussed the data security which the application user has shared during online payments.	In this research paper, the author answers specific questions related to online payments security and discussed different ways to reduce the security threats associated with online payments.
[27]	The paper investigates and increases awareness associated with different electronic payment systems (EPS), including security considerations, challenges, and advantages.	The author conducted a detailed survey regarding all aspects of EPS after analyzing the existing research studies related to online payment systems.
[21]	The author discussed distributed systems and their regulatory compliance related to this approach which is not decentralized yet.	For instant payment systems, the author reviewed some distributed protocols to find the possibility of effectively syndicating distributed systems with centralized services in the mobile payment system.
[28]	With the case of Mobile Payment Technology, the author focus on identifying different technological trajectories in the ecosystem (technological). This research aims to provide a path to develop and integrate the primary services to categorize Technology Evolution (TE) with the help of the Mobile Payment landscape.	The novelty in this research is finding the technological evolution with the help of patent citation and social network analysis. The case of the Mobile Payment Technology ecosystem is analyzed quantitatively.
[29]	The author focused on innovations and new attempts or dominant systems to improve the electronic Mobile Payment System (MPS).	This survey consists of a review of its dominant system and present cart transactions (CPT). At Cambridge University, several types of research are conducted to designate different attacks against authentication methods in MPS.
[30]	The research study aims to analyze and examine the effects of consumers' and consumer preferences for MPS and features of the marginal usefulness of biometric and mobile payments.	Based on the study results, theoretical effects for mobile payment consumer preference and proposed different market strategies for the dispersal of main next-generation MPS from different aspects are analyzed.
[31]	The objective of the author is to analyze the factors that affect users' intention in the Mobile Payment System and the status of Near Field Communication in the transportation system. A widespread review of scientifically collected works validates the progress of interactive model that clarifies the intention of near field communication MPS with the help of structural equation model (SEM).	To achieve the objectives of the research, a survey was completed with 180 mobile payment users. The study results show that perceived risk, effort expectancy, service quality, and satisfaction define the persistence to use MPS.
[32]	The study compares the different factors that determine consumer acceptance quick response(QR), near field communication (NFC), and short message service (SMS) in MPS.	To achieve the objectives, the intention to use mobile payments, a comprehensive review of literature is necessary to improve the behavioral model. The novelty and results of the study lie in the preparation of different behavior rendering given by MPS users to each planned payment application.
[33]	The research study focused on the urban consumer's perception and attitude towards digital MPS.	A convenient survey was conducted to achieve the research objective among 100 urban respondents with an interview schedule. The ranking method, independent sample t-test, one-way Enova, and percentage analysis are used in this study.
[34]	The author reviews the E-MPS in E-Commerce.	This study aims to analyze the available literature related to e-payment and e-commerce to underline the possibility of e-payment and identify the research gaps, and for future studies, the methodology of previous researchers is recommended.

only about using mobile devices to access online payment services. While the mobile version of the service may have similar functionality, the design and implementation of mobile payments are also different due to different methods and structures. Numerous factors boost MPS evolution in developing countries. Following are some of the factors.

1) SOCIOECONOMIC CONDITIONS

The lack of cash alternatives is the most critical factor fostering MPS growth in emerging developing economics countries [35]. Maximum people in developing countries do not have to account and do not have a credit card. Well-developed mobile payment applications with the advantage of low fees for money transfer services make MPS attractive [36]. People moved towards the mobile banking system in almost all countries to save their valuable time and avoid getting robbed.

2) COST EFFICIENCY

In developing countries, most transactions executed online are very low in terms of value, but they are very high in volume [37]. Introducing a new bank branch is infeasible because of massive initial equipment, investment requirement, infrastructure, and well-trained HR included security staff. Bank without different branches looks appealing because it utilizes local infrastructure and leverages local resources and human resources and equipment and resources, including agent shops and mobile phones. Mobile Payment Systems (MPS) are reflected as valuable because of their low-cost investment, no infrastructure, and very low memory in the phone. The fee for a usual payment transfer is almost 1% in all mobile payment systems. E.g., the fee for sending money through Wizzit and MTN in South Africa (SA) is almost US$0.05. However, before the Wizzit and MTN payment system, the average fee is almost US$30 to US$50 for cash delivery.

3) DIFFUSION OF MOBILE PHONES

As cell phones become cheaper, financial systems are still relatively limited, and Mobile Payments (MP) are more convenient [38]. In most countries, individuals may have one or more cell phones. Sub-Saharan Africa has more families with more cell phones than sustainable electricity or drinking water resources.

4) CONVENIENCE

In advanced countries, MP is more suitable. People can pay or withdraw money without leaving their homes, which will significantly save their time and cost of the expensive fees [39].

5) LATEST INITIATIVES

On the other side, many factors limit the growth of MP. Non-governmental organizations and international organizations (e.g., IFC, the World Bank, GSMA, Gates Foundation) have proposed new initiatives to promote and facilitate MPS implementation. For example, M-PESA Kenya was launched and developed by Safaricom and Vodafone with help from UK's Department for International Development. Pakistan

telecommunication (PTC) (Easypaisa) received a $ 6.5M grant from Gates Foundation in 2012.

B. FACTORS LIMITING MP DEVELOPMENT

Several factors are limiting further MP development as follows.

1) HEAVY RESTRICTIONS AND REGULATIONS

This is the most destructive factor in the development of mobile payments. Pressure on banks plays a key part in the ecosystem that decreases the development of MP. Unfortunately, compared to technological advances, most mobile payment methods are changing slowly [36].

2) LIMITED COLLABORATION

In most situations, non-cooperation is an obstacle to the ecosystem. For example, M-PESA has worked with commercial banks for five years to ensure that their valuable customers withdraw their money from ATMs and banks. Collaboration is very significant as most customary banks do not implement to handle MP.

3) UNDERDEVELOPED ECOSYSTEM

Lack of standards, undeveloped infrastructure of systems, limited mobile resources, and saturated telecommunications networks (including disruptions) prevent developing countries from launching Mobile Payment Systems (MPS) [40]. In some situations, interoperability concerns and a specific type of broker are needed to solve the trust problem and reduce the chicken and egg problem.

4) SECURITY PROBLEMS

Cybercriminals' activities are more in developing countries. First, they often lack an adequate legal framework and implementation tools to fight cybercrime. Secondly, occasionally customers may not know, and their attention is very little to security problems.

Given the various influences that drive and delay the development of MP, all critical factors in the ecosystem must be focused on the longstanding goals of the MPS. Of course, the utmost important objective of any MS is to improve competence conducive to financial development. MP is an alternative to financial transactions and specializes in small payments that are not in cash. However, it remains to be seen whether the key players in the development and implementation of the technology are willing to make large-scale commitments [41].

Given the various influences that drive and delay the development of MP, all critical factors in the ecosystem must be focused on the longstanding goals of the MPS. Of course, the utmost important objective of any MS is to improve competence conducive to financial development. MP is an alternative to financial transactions and specializes in small payments that are not in cash. However, whether the key players in developing and implementing the technology are willing to make large-scale commitments remains to be seen. MPS leads to new marketplace ecosystems, including mobile operators, card operators, retailers, service providers, banks, hardware vendors, trusted service managers, and technology vendors. Several critical regulatory issues emerged, including electronic money and payment systems, consumer data protection, MPS principles, and confidentiality. Mobile payment systems are used for interpersonal transfers (P2PT), handling small purchases, paying bills and expenses, and purchasing specific goods or services. Almost all mobile network operators that provide mobile payment systems operate in the few countries/regions they are located in, thus facilitating international transactions and remittances [41].

There are no separate laws for MPS in several cases, especially in undeveloped countries. On the other hand, depending on the types of mobile, payment, retail and convergent value chain technologies described and classified above, the program is multifaceted and extensive [41]. The bond structure is unmoving in its beginning but applied in all areas and at all system levels. With the development of technological threats and economic and financial benefits, mobile payment systems began to develop. The regulatory issue of mobile payments is new for at least two reasons. First, it summarizes the different areas of data privacy, e-money, ICT, mobile services, e-payments, user protection, and information and rules and regulation. Second, there are some specific problems with innovation, namely the interpretation of electronic money and the oversight of payment systems.

C. MOBILE PAYMENT SYSTEM KEY ATTRIBUTES

All MPS provide greater convenience of using mobile devices to process electronic payments [42]. However, it should be noted that because they perform many functions in a universal payment system, mobile payment services have different features that will affect the preferences and decisions of the user. Therefore, mobile payment services have complex features, including a combined merchant visits, identity verification, and payments. Table 3 presents the key attributes of the mobile financial system (MFS).

It is still significant to explain the concept of MPS, containing mobile banking (MB), mobile payments (MP), mobile wallets (MW), and mobile currency (MC). Considering the above facilities are the main research encounter in mobile money transfers [43]. MB mentions providing banking services through mobile communication devices, including financial transactions (for example, money orders and bill payments) and non-financial business transactions (for example, balance surveys). Some researchers believe that the functions of MB and MC intersection [44].

While MB is primarily seen as a straight link between consumers and banks [45], mobile payments are categorized as a service that affiliated service suppliers can use without the involvement of banks. Mobile payments are common and generally refer to any payment that uses a mobile terminal to confirm and authorize a payment transaction [46]. Alternatively, mobile wallets are defined as progressive

TABLE 3. Mobile financial system.

Mobile Financial System	Description
Mobile Currency	MC is a currency that can be opened and used by an MP deprived of a bank account [47].
Mobile Payment	MP is a payment system used by an MP to authorize, initiate and confirm a transaction [46].
Mobile Wallets	MW is a mobile application that can replace physical wallets and include the following features: The ability to store information about payments, membership cards, and membership cards, and other marketing plans [46].
Mobile Banking	MB means providing banking services via mobile phones, including financial and non-financial transactions. Wireless device [44].

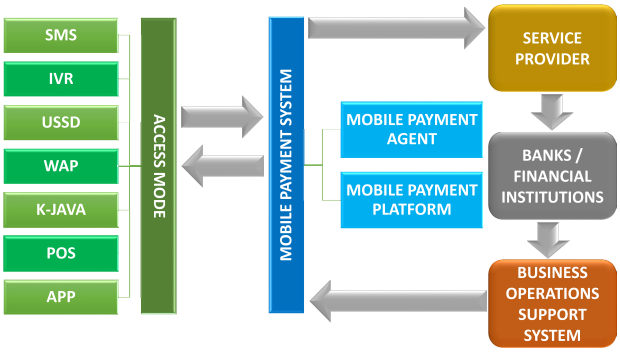


FIGURE 4. Structure of MPS.

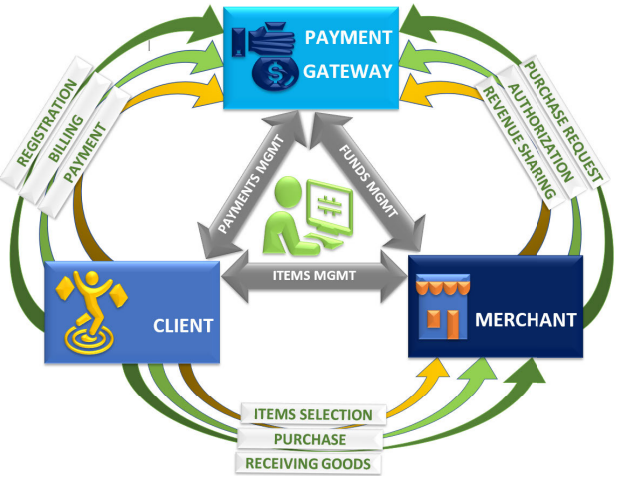


FIGURE 5. Primitive transactions.

mobile applications that replace physical wallets and have numerous functions like storing payment information and affiliation card and executing transactions. Finally, mobile currency is a currency that can use and accessed via an MP. Especially since it allows users to run a business (e.g., money orders) without a bank account, it is extensively used among rural inhabitants and cannot use traditional financial institutions. [47].

D. M-PAYMENT STAKEHOLDERS AND ENTITIES

1) STAKEHOLDERS IN MPS

Many diverse stakeholders in implementing M-Payment include consumers/clients, merchants/providers, mobile network operators (MNO), mobile device manufacturers, financial institutions, banks, software, and technology providers. The government is the stakeholder in the M-Payment implementation process. Each stakeholder has different incentives, roles, and strategies. Sometimes these interests and strategies between different stakeholders conflict, e.g., the network provider would like to maximize revenues through each m-payment transaction, whereas customers and merchants would like to minimize costs for each M-Payment transaction. In [48], the authors highlight the critical finding that mobile payment method depends on their providers to connect the merchants and consumers to the degree that satisfies the stakeholders.

2) COMMUNICATION ENTITIES IN MPS

For the payment process, there are multiple entities (as shown in Table 4) that perform their role. Figure 6, [49] shows the entities that communicate in mobile payment process. The entities can be less or more according to the protocol.

Steps involved in M-Payment process

1) Client requests a merchant for the payment.
2) Merchant requests to the payment gateway for the transaction amount to be a deposit.
3) Client request to the payment gateway for checking the deduction amount from the account.
4) Payment clearance is held in the payment gateway.
5) Payment gateway response to the client request in the form of rejection or approval.
6) Payment gateway response to the merchant request in the form of acknowledgment receipt.
7) Merchant gives the payment receipt to the client and confirms the transaction.

Figure 5 represents the model of primitive transactions in which the client makes payment to the merchant. The payment value is subtracted from the client's account at the issuer's request by the payment system, and then at the request of the acquirer, the merchant transfers/adds the value from the payment gateway to its account.

III. MOBILE PAYMENT SYSTEM SECURITY MECHANISM

MPS security mechanism includes: Encryption technology, authentication, and a firewall [50].

TABLE 4. Entities that involve during mobile payment process.

Entities	Description
Client	An entity who wants the transaction
Merchant	An entity that has products or services to sell. It could be a computational one (like a standard webserver) or a physical one.
Payment Gateway	another entity acts as an intermediary between the acquirer/issuer on the bank's private network side and the client/merchant on the Internet for payment clearing purposes.
Issuer	The client's financial institution manages the client's account and affords the electronic payment instruments to be used by the client.
Acquirer	The merchant's financial institution manages the merchant's account and verifies the deposited payment instrument.

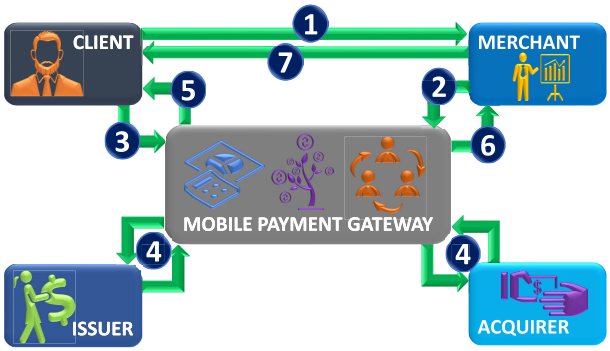


FIGURE 6. Entities involvement in M-Payment process.

A. ENCRYPTION TECHNOLOGY

Encryption technology includes Symmetric encryption and public-key encryption.

1) SYMMETRIC KEY ENCRYPTION (SKE)

SKE system uses a common key to encrypt messages, which means both sender and receiver will hold a common key for encryption and decryption. Before transmission of data between both parties, the common key is shared on the secure channel between both entities [51]. Exchanging keys between both entities is important for encryption processes. Short size and weak keys are easily attacked as opposed to longer keys. Symmetric encryption is still commonly used in insecure data communication.

2) PUBLIC-KEY ENCRYPTION (PKE)

PKE system is a type of asymmetric encryption because the same key is not used to encrypt and decrypt the messages. In the PKE system, two different keys are used, called public and private key [51].

3) COMPARISON BETWEEN SKE AND PKE

There are numerous differences between the SKE system and the PKE system. Table 5 presents the comparison of the SKE and PKE.

B. AUTHENTICATION

Authentication included: Digital signature and certificate authority.

1) DIGITAL SIGNATURE

Digital signature (DS) is used to verify the origin of the received text and prove whether the received text is without any changes or not. To certify the availability of DS, public keys infrastructure (PKI) is frequently used. It suggests a complete set of security assurance and follows different public key encryption standards for different sectors like online banking, e-banking, e-government, and e-commerce securities [52].

2) CERTIFICATE AUTHORITY

The Certificate Authority (CA) is a trusted organization that publishes and manages network security PKI and credentials for message encryption. As part of the PKI, the CA will use the registry for verification. Users have the right to verify the information in the digital certificate provided by the applicant. Suppose RA (Register Authorities) verifies the applicant's data and issues a digital certificate. Users are responsible for distributing and revoking certificates in a communication system. Depending on the PKI, upon request, the certificate may contain the holder's public key, the certificate, the name of the certificate holder, and other information about the holder of the public key [53].

C. FIREWALL

The firewall can simultaneously protect the system /local network against network-based threats. The firewall allows access to the outside world to the local network. In most scenarios, a firewall is necessary because it is difficult to equip all devices with different security devices. Typically, the firewall is inserted between two networks.

IV. AUTHENTICATION METHODS IN MPS

Authentication methods are widely used to test user identity in mobile transactions as the user identity is required to execute transactions [54]. Some of the authentication

TABLE 5. Comparison of encryption methods.

Characteristics	Symmetric Key	Public Key
Several keys are used for encryption, and decryption	The same key is used for encryption-decryption	Two different keys are used for encryption and decryption.
Speed of encryption and decryption	Faster than public-key encryption	Slower than symmetric key encryption
Size of ciphertext	Usually less than or same as the plain text	More than plain text
Key exchange	A big problem	No issue
Key usage	Used for confidentiality but not for digital signature	Used of confidentiality and digital signature as well

methods are knowledge-based authentication verification, object-based authentication verification, and biometric authentication. With knowledge-based authentication, users use a personal identification number (PIN) or password to validate their identity [55]. This is based on well-known traditional authentication methods, so they have fewer security issues. Physical tokens (such as smart cards) are used to perform object-based authentication. While objective knowledge-based methods can create inexpensive and straightforward authentication systems for various computing applications, they can close security vulnerabilities. In addition, the above two methods are likely to be lost or forgotten by the users, which can be an intellectual burden for application users [56].

To overcome the limitations of the above traditional methods, some advanced authentication systems have been developed that provide consumers with adequate security [57]. Biometric methods based on user personal identity (i.e., Physical Characteristics) have been effectively applied to protect and verify users' identities. Identity verification based on human-specific biometrics (such as fingerprints, voice, or iris) is unlikely to be easily stolen or transferred. [58] Presents the advantages of the biometric authentication systems included: improved account security and reduced loading. Biometric technology has its limitations. Because of the complication of high-quality images, many factors in a biometric system will reduce user identification accuracy [59]. Physical issues like wet surfaces, dirty fingers or scratches are familiar illustrations that can delay biometric authentication. In addition, the biometric system also has some privacy issues related to users' identity management. However, there is also an advanced ''Knowledge Based'' authentication method. To provide more security features, graphical prompts (such as design drawings) have also been proposed as a substitute to the above authentication methods [60]. A recent study found that using different e-payment authentication methods will affect users' perception of security and availability of these three authentication types. Therefore, in this study, the method of identity verification was selected as one of the primary resources for creating the preference structure of mobile payment users [54].

A. TYPES OF AUTHENTICATION FACTORS

Three types of authentication factors, namely, single-factor authentication (SFA), two-factor authentication (2FA), and multi-factor authentication (MFA), can be understood through the definitions proposed by the research of [61] and [62]. colorThey proposed that a process allowing individual users to seek access from authenticating parties for attestation of their personalities with the utilization of single attribute associates with their identifies is termed as Single-Factor Authentication (SFA). An example of such an attribute would be the use of a PIN for unlocking cell phones. The user-friendly and straightforward nature [63] of this authentication type made it a preferable choice for many companies; however, its vulnerability to various forms of attacks [62] made it unsuitable for application in financial institutes.

The authors in [62] proposed Two-Factor authentication (2FA) for accessing MPS applications. 2FA included a double security check for accessing and using MPS applications. Authentication attributes include knowing something personal or possessing something personal that can be associated with one's personality. Hence, attackers are bound to be aware of two identifiers to get the same authentication as the original users in 2FA. This particular feature of 2FA makes it acceptable and applicable to financial institutions. However, this type has loopholes, leaving it vulnerable to a MITM attack, eavesdropping, and Trojan horse attack. Furthermore, it has its limitations when considered for its effectiveness against phishing [63].

For defining the third type of authentication factor named Multi-factor Authentication (MFA), the authors in [62] describe that it involves users seeking requests for access from authentication parties through attestation of their personality with multiple attributes. Biometrics are used along with ownership and knowledge as an attribute by MFA. MFA's higher level of security makes it a better choice for various critical services and computing devices. Physical separation of authentication factors from the user device can allow MFA to be more successful. The addition of biometric factors makes MFA achieve improved identity proof resulting in more secure systems [63], [64].

V. CYBERATTACKS ON MOBILE PAYMENT SYSTEM

Different types of attacks on MPS can come from unauthorized malicious users. Below are some of the possible attacks on MPS.

The first attack is targeted at the users of mobile money. It includes accessing the PIN of users via shoulder-surfing when it is unmasked PIN of four to five digits [65]. Access to this PIN can enable attackers to make fraudulent transactions.

Brute force attacks can also be performed by attackers considering the straightforwardness of the PIN [66]–[68].

The second type of attack involves comprising of money communication channels, where the hacking and controlling of MMS traffic and manipulation of accounts for making transactions can be made possible [66]–[68].

The third type of attack is at the server of the mobile money app. Availability of server to both mobile money agents and users is suspended when such attack is carried out at server. As per the findings of [66], attackers divert fake traffic to mobile money servers resulting in it being overwhelmed, which eventually leads to blocked requests from mobile money agents and users. It can also include installing malware on the mobile money app server for deducting some amount from wallets of mobile money agents and users for deposition into the attacker's account without letting these users or agents discover the transaction [69].

The fourth point of attachment is the IT administrator. The administrator's computer can be hacked by an unauthorized person making it inaccessible by changing its credentials. Mobile money agents can be considered as another attack point. The PIN of the commission agent can be stolen by an attacker using shoulder surfing techniques. Attackers can also practice giving the wrong PIN repeatedly while making transactions to access agents' PINs. [70] and [71] Identified adversaries may give wrong phone numbers repeatedly to obtain the PIN of agents and use it for gaining unauthorized access to the accounts of agents.

Bank's server provides another attack point for adversaries. A distributed denial-of-service attack (DDoS) is made in such cases to create the unavailability of a bank server to the mobile money user trying to make a transaction.

Notification message channels where messages can be modified creates another attack point for malicious users. Adversaries may hack the communications channels of the notification message and make changes in the message as per their requirements while sending the modified versions of these messages to the intended users [72], [73].

A. ATTACKS AGAINST PRIVACY

[74] defined privacy as the right of users to have freedom from intrusions and infringements by other users. In mobile money, privacy attacks include the compromised PINs of the users for illegal access to their financial assets and information details utilized in unauthorized transactions. Stealing of user information can result in a problematic situation for not only the user but also for the economy as well [74]. Illegal access to the mobile money database containing users' financial information can allow attackers to update or delete records using the stolen PINs.

Moreover, a variety of user-related information can be stolen when an attacker gets access to mobile money database [74]. Personal information such as email addresses, mobile telephone numbers, NIN, and even names of users and agents can be compromised, failing privacy safeguards [74]. Unscrupulous insiders may end up abusing highly sensitive data after gaining control and access in this way. Attackers can do so with the generation of a databank to give control and access to personal information. There are situations in which some users request the agents for assistance in performing transactions, and they end up sharing their PINs with the agents [75]. It raises the bar for the required level of protection to agents and mobile money users against unauthorized access.

B. ATTACKS AGAINST AUTHENTICATION

According to [76], an authentication attack is a crime in which the mobile money authentication process is subjected to exploitation when a brute force attack is being carried out against the PIN. Various attacks are included in this form of attacks, such as Trojan horse attacks, phishing attacks, social engineering attacks, spoofing attacks, masquerade attacks, replay attacks, and impersonation attacks. The identity of a user is forged by an attacker impersonating an authorized user in this form of attack. An attacker assumes the identity of a legitimate user in an impersonation attack [70], [71], [76], [77], whereas entire communication is subjected to eavesdropping in replay attack before intercepting [78]. In a masquerade attack, the PIN and SIM card is acquired by the users.

Moreover, an attacker pretends to be a mobile system administrator in a spoofing attack. When users are manipulated for them to give up their personal information, a social engineering attack is said to be launched [79]. Similarly, a phishing attack involves deceitful attempts by adversaries for accessing personal information needed to impersonate a legitimate user in the system [76]. Another method of compromising an authentication system involves using Trojan software as a virus to access users' personal information.

C. ATTACKS AGAINST CONFIDENTIALITY

Attacks on confidentiality involve eavesdropping on the communication channels between the application server and mobile money users for tapping information like PIN of users that can be used for impersonation or making unauthorized transactions. The four types of such attacks include guessing attacks, brute force attacks, eavesdropping, and should surfing attacks. Attackers secretly hear the communication channels in the eavesdropping attacks by taking advantage of the lack of security of the network communication. The plain text form of transmitted data is commonly vulnerable to such attacks [80], [81].

For brute force attacks against confidentiality, the adversary can guess the mobile money agent or user's PIN to access the mobile money account. Despite being very simple, such types of attacks have shown a high rate of success [70], [71], [76], [77]. When an adversary sees a mobile money PIN during authentication, a guessing attack is being launched. Shoulder surfing attack also comes under the type of attacks against confidentiality in which the adversaries acquire confidential data and PINs simply by looking over the

shoulder of the victim as they make transactions [77]. [82] discussed one of the approaches that can be utilized to extract useful network information to identify the details of the endpoint of the communication parties on the local network.

D. ATTACKS AGAINST INTEGRITY

When user information is accessed and modified in the MMS, the integrity of user information is compromised. They can be categorized into insider attacks, salami attacks, and MITM attacks. An intruder intercepting the communication between various agents (including users) in the mobile money application network performs Man a middle attack. Sitting between the mobile money user and MMS, the attacker makes them believe they communicate in the MITM attack. [81] and [68] showed that an attacker could gain control over the entire conversation when a MITM attack is being launched as the content of the conversation is modified by the attacker at both ends.

Employees of financial institutions can conduct salami attacks and insider attacks against the financial institutions. Like a Trojan horse, a salami attack involves installing malicious software to a financial institution system, allowing adversaries to withdraw money from users' accounts, depositing it in their accounts. Both external and internal adversaries can launch salami attacks in which small deductions are made to user wallets as the software allows modification of some details in the system [83]–[85]. [86] and [87] highlighted the fact that a high degree of risk of money fraud comes from the employees of the financial institutions who are aware of the security protocols and MMS in the system. MMSP employees with sufficient knowledge about the organization's security practices can be involved in the insider attacks identified by [75], and [86].

E. ATTACKS AGAINST AVAILABILITY

When the bank server or application server is suspended for agents and mobile money users by an adversary on purpose, an attack is assumed against availability. Services are rendered unavailable by adversaries in this type of attack using various techniques. Mobile theft, DOS, and distributed denial of service (DDoS) attack come under this category. DDoS and DoS are launched when adversaries send fake traffic to overwhelm servers to block legitimate traffic or requests of users [76]. Such attacks aim to flood mobile money servers with so many fake requests that the server fails to receive and respond to legitimate users' actual requests, making the service unavailable. [67], [76] described mobile phone theft attacks as the type of availability attack in which the mobile phone of users or agents is stolen, and the wallet account of SIM card is made unavailable that can be swapped by the attacker. Service and data access can be lost due to phone theft attacks, as the attacker can take charge of the victim's e-wallet account, resulting in its unavailability to the actual user.

VI. TECHNOLOGIES USED IN M-PAYMENT PROCESS

We have also seen an M-Payment system based on the technology used; it is classified in Figure 7. M-Payment system uses mobile technology for communication between the entities involved in the payment process.

Near field communication (NFC) [88] is a communication protocol that enables communication between two devices. Global system for mobile (GSM) [89] is a standard system for mobile communication. Radiofrequency identification (RFID) [90] uses an electromagnetic field to identify or track tags attached to an object. Short messaging service (SMS) [91] is a text messaging service that is used for communication over the mobile phone. Quick Response Code (QR-Code) [92] is a two-dimensional matrix barcode, which has a label in which information is stored. Bluetooth [93] is a standard for wireless technology; by using this, we can communicate to fix devices over a short period of distance. Identity-based signature (IB-Signature) [94] is a type of PKI in which a publicly known string that represents an individual is used as a public key, e.g., email address, the wireless application protocol (WAP) [95] is a standard protocol used in the wireless network to access information. Universal 2nd Factor (U2F): It is a standard of open authentication which provides two-factor secure authentication.

1) REVIEWED APPROACHES

This study has reviewed multiple schemes or models of mobile payment systems based on different technologies or architectures. Authors in [96] used RFID and SIM, which enables users to use their mobile phone as an ATM card/credit card. By using RFID readers at ATMs, users can withdraw money. Authors in [97] used Bluetooth with Java technology by which users can pay at POS (point of sale) by using a mobile phone. Java components are used here to provide encryption. Authors in [98] enhanced SEMOPS (Secure Mobile Payment Service) model by involving a trusted third party.

Authors in [99]–[101] used GSM technology to implement a secure m-payment system. It provides low-cost architecture by using the existing GSM mechanism. Authors in [100]–[103] used NFC communication, which provides more speed for communication than other technologies. In [101], the proposed scheme also provides user anonymity and the un-linkable transaction to defend against attacks. [102], [104], [105] use QR-Code, which is fast and supports the buy-and-sale process easily and efficiently. In [103] using SMS service; mostly SMS service in mobile communication is used for authentication. In [106], using the SMS based authentication system, an application-based system is proposed in which authentication code can only be accessed by an authorized user, and using IB-Signature, which is simple and less costly, the identity of an entity is used in this technology for authentication or for granting access. Authors in [106] also use the OTP code for securing communication; it prevents the system from replay

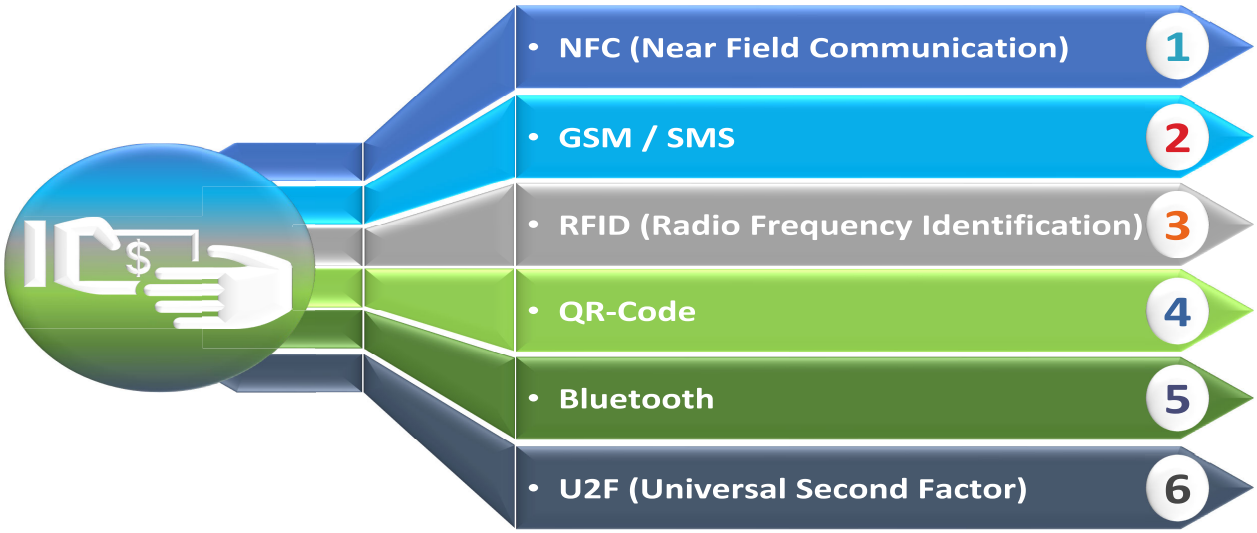


FIGURE 7. Technologies used in M payment system.

attack and uses a password for only one time. WAP or Bluetooth technology is used in [107] which provides fast communication but over a small range of areas. It is for peer-to-peer communication since it costs less. [108] uses SMS for sending a notification, but for transactions purposes, it uses unstructured supplementary service data (USSD), which provides a more responsive service than SMS. In [109], the authors use U2F technology, which is fast and much secure; it performs cryptographic functions with a single touch & generates asymmetric keys. It authenticates both the client and server in a reliable manner so transactions can be done securely. Query processing over encrypted data is the solution to tackle the extra overhead caused by the use of encryption, and such techniques result in remarkable improvements in the scenario where near real-time data processing is required [110].

2) ANALYSIS

The overall average of technological usage of MPS is depicted in Table 3. The proposed research analyzed technologies and found that **SMS is used primarily for MPS**. On the other hand, NFC, GSM, and QR-Code increase payment schemes or models every day. The MPS technologies provide several advantages. NFC provides faster speed; GSM provides several already implemented services that make these models' implementation easy. QR-code is a less costly and straightforward technology used in many mobile payment systems. In addition, U2F is much secure and reliable than QR-code, NFC, and Bluetooth.

VII. SECURITY ANALYSIS OF M-PAYMENT SYSTEMS

This section presents the security analysis of the M-Payments system. Security analysis comprises various services: authentication, mutual authentication, integrity, customer anonymity, and non-repudiation. Figure 8 depicts the overall service hierarchy of the m-payment system. Each of these services is discussed in detail as follows.

3) CONFIDENTIALITY

In [97], confidentiality is provided by using Java components. In [98], [115], the authors use cryptography to provide confidentiality. In [106] OTP and PKI infrastructure are used to provide confidentiality. In [100], GSM security mechanism is used which provide confidentiality via *A*5 and *A*8 algorithm. In [103], [107] confidentiality is achieved by using Symmetric key cryptography to provide confidentiality. Authors in [104] use RSA encryption mechanism to provide confidentiality. In [111], DES and ECC are used to achieve confidentiality. In [105] confidentiality is achieved by using AES and RSA. In [112] secured end-to-end encryption is used to provide confidentiality. In [118], symmetric key encryption is used to provide confidentiality. In [114], RSA encryption mechanism is used to achieve the confidentiality. In [109], Asymmetric cryptosystem is used to provide encryption. In [101] AES is used to provide confidentiality which is a type of symmetric key cryptography. [116] provides confidentiality by encrypting the information using asymmetric keys and the key pair stored in the secure storage [117] to protect from unauthorized access. In [113], confidentiality is achieved by using ECC, which is a type of asymmetric key cryptography.

4) AUTHENTICATION

In [96], authentication is performed by reading the RFID tag, which is embedded in the SIM card. RFID reader authenticates the user in this scheme. In [97], authentication is provided by asking for a PIN and account number. In [99], authors used to control and communicating interface to provide authentication. In [102], authentication is done by using NFC enabled mobile phone and QR-code/PIN. In [100],

TABLE 6. Comparison of reviewed papers on the basis of payment system technology, architecture, communication entity involvement, assumption, advantages and disadvantages of solutions (I).

Ref	M-Payment Based On	Architecture Used	M-Payment Between	Provides	Assumption	Advantage	Disadvantage
[105]	RFID	RFID & SIM	User & POS User & Service provider User can also deposit money	Easy to pay service and ATM/Credit card functionality through mobile	RFID readers are installed at stations, shopping malls, & at ATM,	Flexibility, time, workforce reduction, safety & mobility	Some issues in security & privacy in RFID Chances of unauthorized use are present in case of theft or loss of mobile.
[107]	J2EE and J2ME capabilities	Java, Bluetooth	Payment server & mobile clients	Confidentiality and Authentication	MIDP application is uploaded to client's mobile	It overcomes the API and technical limitations, as well as security consideration	As the number of clients increases the delay (milliseconds) will increase over Bluetooth environment
[111]	Existing models	SEMOPS & trusted third elements	Customer & Merchant	Privacy & Non-Repudiation	All parties possess certificates among each other	It introduces trusted third elements & follows new Mechanism to achieve privacy & non-repudiation	Difficult to implement.
[112]	Multiple layers	SMS, GSM	Consumer & content provider	Security & High Scalability	-	It provides low cost and technical requirement, high scalability, and security	The system required to be more simplified, improve the security & application of digital signatures.
[109]	Scenario for m-payment models	NFC, QR code	Customer & Merchant	Speed & Security	-	For speed, transaction is initiated by merchant because he has more reliable & continuous connection with 3rd party	For every new purchase, there will be authentication by merchant's involvement which can make him busy and it can affect his availability.

TABLE 7. Comparison of reviewed papers based on payment system technology, architecture, communication entity involvement, assumption, advantages and disadvantages of solutions (II).

Ref	M-Payment Based On	Architecture Used	M-Payment Between	Provides	Assumption	Advantage	Disadvantage
[106]	Identity Based Cryptography (IBC)	IB Signatures and One Time Key	Consumer and Merchant	Privacy and Security of transferred data	-	IBC framework is simple and less costly	Higher number of cryptographic operations
[100]	GSM	NFC and GSM	Point-of-Sale (POS) and the customer	Security for low-value payments, customer anonymity and ubiquitous implementation	Secure channel between a payment gateway and shop POS	Re-using existing GSM security mechanisms Payment is same as paying by debit or credit card.	-Short length of the encryption key. -Merchants need to register themselves with mobile operator -protocol is complex as compared to m-payment via SMS or WAP
[113]	SMS	SMS, WAP or Bluetooth and J2ME.	Payer's or Payee's bank	Secure M-Payment for macro transactions -less encryption or decryption operations	Trusted payment gateway is involved between payer's and payee's banks	This scheme shares payee's financial data with banks only	If mobile got stolen and PIN got also leaked then there are chances of financial loss
[114]	PKI	QR-Code and PKI	Client and merchant	Additional layer of security form-payment systems	Trusted the third party is involved in securing encryption keys and in ensuring legitimate users	This scheme uses RSA which is considered as strongest asymmetric encryption system	For stronger security longer key pair is required which leads to the larger size of QR code
[115]	3G	3G, SMS and IVR	Client and server (Mobile Payment Platform)	Intelligent travel design by using m-payment system	-	By using this user can pay fines, insurance amount or can query traffic violations rules etc	Initial connection in this system takes longer time
[116]	2D Bar Code QR 2D Bar Code	Point-of-Sale (POS) and the customer	Advantages to support buy-and-sale products and services base on 2D Barcodes	Trusted third party authentication server is used as Certification authority	-	Products can be traded anywhere, anytime Easy to use Reduce user input	Computations are little complex
[117]	SMS	SMS	P2P Peer-to-peer	It provides features like security, privacy, speed, and less cost	-	Money transfer can be done by transmitting mobile number only	Huge number of different device OS and development environment may prevent Support for all devices

the triple authentication mechanism is ensured by using the challenge-response protocol. In [107], authentication is provided by using SMS and secret key. Authors in [111] ensured authentication by using signature schemes (DES and ECC). Authors in [112] used short-codes to provide authentication. In [118], Isomorphic shapes are used for authentication.

5) MUTUAL AUTHENTICATION

In [98], [106], [113], payment requests are signed by signing key (digital signatures) of both client & merchant to achieve mutual authentication. In [104], mutual authentication is ensured by using the RSA-PKI mechanism. In [105], RSA-digital signature is used to provide mutual authentication. In [114], identity-based signatures are used to achieve mutual authentication. In [108] mutual authentication is achieved by using mobile wallet number and PIN. In [109], mutual authentication is provided by using asymmetric keys, valid username, and password. For authentication, [101] uses session-key and challenge-response authentication. To ensure mutual **authentication** [103], uses secret key and PKI. In [116], authentication is provided by using digital signatures. In this scheme, mutual authentication is only between the user and the bank.

TABLE 8. Comparison of reviewed papers on the basis of payment system technology, architecture, communication entity involvement, assumption, advantages and disadvantages of solutions (III).

Ref	M-Payment Based On	Architecture Used	M-Payment Between	Provides	Assumption	Advantage	Disadvantage
[118]	Cryptographic Protocol Shape Analyzer (CPSA)	CPSA	Merchant and payment gateway	Payment mechanism ensuring accountability and un-linkable anonymity less number of cryptographic operations	Customer browses through the merchant website	Customer has an option of making payment using cards of different banks	Limited to a maximum of two gateways
[114]	Traceable signatures, identity-based signatures, anonymous signatures	Signatures	Ternminal and passenger	Provides mechanism to protect passenger's privacy	Off-board terminal trusts on-board terminal	It can be applied to off-line mobile payment systems	-
[108]	Unstructured Supplementary Service Data (USSD)	USSD and SMS	User to agent and agent to user	Secured transaction by using two layers of authentication	Mobile wallet number is same as mobile number and there is large no. of agent points across the country	Mitigate human error and prevent cyber-frauds	Does not consider confidentiality and integrity aspect
[109]	Universal 2nd factor (U2F)	U2F, USIM	User to server	Secure mutual authentication protocol for m-payment systems	-	Provides a reliable service and protect user's account information and privacy	In registration process, it will take time since it is using asymmetric cryptosystem
[106]	NFC	Wi-Fi, 4G, GSM NFC	Bank to bank (POS)	Enhance the security of the Europay, MasterCard, and Visa (EMV) exchanged messages	Mobile network operator (MNO) is trusted by NFC enabled Mobile	Adds a security layer to EMV and ensures confidentiality and mutual authentication	It will be failed if POS entity is dishonest
[118]	NFC	NFC	User and Trusted service manager (TSM)	Secure protocol which is compatible with EMV	TSM and Bank own their key pairs of a PKI cryptosystem	User can perform transaction without disclosing his identity.	Requires a high computation power for TSM and bank
[116]	NFC enable phone	NFC and trusted third party	User and Merchant	User anonymity	-	Un-linkable anonymity to user	-
[119]	SMS	-	User and bank, bank and gateway	Secure transaction with formal technique	-	Less time take for key generation and encryption decryption, and scheme security is verified by tools	Only for Android and Java 2 Micro Edition device
[115]	Application Based	Mobile transaction authentication number system	User and Bank	Application-based system that is comparatively more secure than SMS based system	Attacker can get access to web and SMS at the same time	More security than SMS based MTAN	Less efficient than MTAN

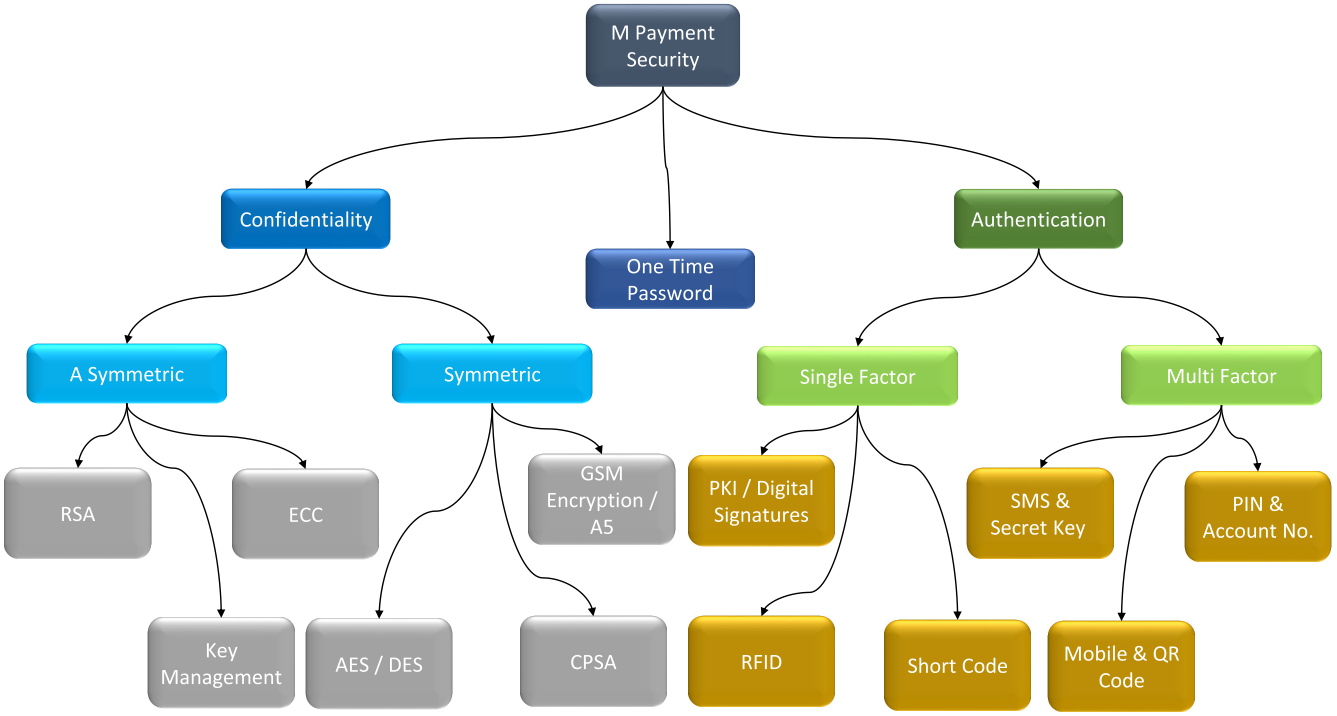


FIGURE 8. M-Payment security.

6) INTEGRITY

To ensure that the data is not tampered during transaction, authors in [100], [101], [106], [109], [113], [114] used hash packets and verified the hash. Authors in [107] use a private banking network and secure payer confirmation to ensure integrity. In [104], integrity is ensured by using QR-Code. In [105], RSA-Digital signature algorithm is used to ensure integrity. [100] achieved the integrity by message authentication code (MAC) that is embedded in the ciphertext. In [116], the information is encrypted with shared key among bank/user and signed with user's private key that protects the information from unauthorized modification.

7) CUSTOMER ANONYMITY

In [98], there is no need to get registered to the merchant or any 3rd party before or during the transaction, which

TABLE 9. MPS technology specific categorization.

Technology	Papers	%
NFC	[102], [103], [101], [100], [106], [116]	28.57
GSM	[96], [99], [100], [101]	19.04
SMS	[99], [100], [107], [111], [112], [108], [113], [115]	38.09
RFID	[96]	4.76
QR-Code	[102], [104], [105]	14.28
Bluetooth	[97], [107]	9.52
U2F	[109]	4.76

ensures the anonymity of the client. In [100] the client's long-term ID is not revealed to the merchant, which ensures the client's anonymity. In [112], the anonymity of consumers is ensured because it only requires the consumer's mobile number or short-code provided by them-payment application service provider. In [118], a customer's identity is dynamic and updated frequently to ensure the anonymity of a customer. In [114], the client's anonymity is ensured by hiding session and transit information. [103], [116] achieve anonymity by using virtual accounts for clients whom the bank assigns. [120] proposes a novel approach of ensuring privacy, confidentiality, and authentication using a hybrid scheme for location and payment authentication.

8) NON REPUDIATION

In [116], Non-repudiation is ensured by using the signing key and timestamp. In [106], IBC-signatures are used to ensure non-repudiation in their scheme. In [107], three factors are used to prove non-repudiation of the client (by checking the status response of the client, session key, and the offline PIN). Authors in [105] used RSA-digital signature to sign transaction information which ensures non-repudiation of transactions. Authors in [109], [113] used signatures to ensure the legitimate user and non-repudiation. [101] ensured the non-repudiation by hashing the transaction data with the shared key. In [121], authors explore data sharing and privacy for patient IoT devices using block-chain. In [116], the secure storage of NFC generates the key pair (public, private) for a virtual account, and a private key signs all messages during the transaction process, which ensures non-repudiation in their scheme.

The overall security features provided by each paper in our study are described in Table 10. It tells us that all the systems we have reviewed ensure authentication, and most of them also provide encryption. The main aspects of each payment system are encryption and authentication; without these two aspects, no system can be said to be secure enough. Integrity and registration of clients or merchants have also got much importance and value while designing any payment system.

VIII. CHALLENGES AND FUTURE WORK

Due to the increase in technology used worldwide to ease daily life activities, mobile payment systems also emerged rapidly for the same reasons. Tasks that take hours to perform by visiting the banks are now at the fingertips using smartphones and allied payment infrastructure in digital forms. This ease also brought some related issues,

TABLE 10. Security specific categorization of reviewed research papers.

Security feature	Papers	%
Confidentiality	[97], [98], [100], [101], [111], [112], [103], [104], [105], [107], [106], [109], [118], [114], [116], [113], [115]	80.09
Authentication	[96], [97], [98], [99], [102], [100], [101], [103], [104], [105], [107], [111], [112], [108], [118], [106], [109], [114], [116], [113], [115]	100
Integrity	[100], [101], [103], [104], [105], [107], [106], [109], [114], [116], [113], [115]	57.14
Mutual Authentication	[98], [101], [103], [104], [105], [108], [106], [109], [114], [116], [113], [115]	57.14
Customer Anonymity	[98], [116], [114], [118], [112], [100], [103]	33.33
Non-Repudiation	[98], [101], [105], [107], [106], [109], [116], [113]	38.09

the most dangerous of which is the threat of malicious actors hacking the payment system to steal money. The recent hacking of block-chain-based cryptocurrency exchanges, which were previously considered the most secure digital payment system, rings the bells that the hackers circumvent ways to bypass the securities in place. This new battleground between the good and the bad for enhancing and ensuring the security of mobile payment systems against emerging threats is an affluent area to explore in the future.

In any field, there is always the possibility of enhancements and improvement. In the future, we intend to focus on understanding the preferences of consumers and the reasons to utilize or not utilize a specific technology-enabled service as it is vital to design viable services that generate value to consumers and the other stakeholders of an ecosystem. The usage of mobile phones is high, and it is in almost every person's approach. Most of the work or daily transactions or communication is done through a mobile phone; that is why many companies introduced their services for mobile phones. Mobile payment methods are also available nowadays, but it needs more security than other mobile phone services.

Mobile payment solutions will increase the user base, which is already sufficient compared to other traditional methods. This increase will ultimately result in a load on the network infrastructure, which is the backbone of the success of such solutions. Advancement in next-generation networks and their impact on mobile payment solutions will be another research area to explore. Further, research can be done on current bottlenecks resulting in lesser mobile payment solutions and remedial measures using network advancements.

This research has some practical and theoretical limitations that may provide valuable findings for future research. For example, we do not consider the potential impact of digitization on mobile payment systems, making behaviors more complex than those resulting from modular reorganization alone. Our goal is to record dynamics that cannot be found in developed countries. We hope our findings can be applied

to other mobile payment systems in emerging economies. However, future comparative studies using larger samples or more extreme cases will confirm the extent to which our results can be generalized. Since all cases are based on mobile network operators, future research on banks or third-party models will help discuss mobile payment systems in the literature.

IX. CONCLUSION

This paper discussed various payment schemes and their usage, technology, and provided security mechanisms. Most payment methods are account-based payment systems, and their main focus is on security, privacy, confidentiality, and authentication. We present an overview and discussed different components of MPS. We presented a detailed survey of the existing MPS structure and its limitations; provided detailed history, development, and deployment of MPS. We discussed different aspects of MPS, including socioeconomic conditions, cost efficiency, diffusion of mobile phones, convenience, new initiatives, heavy restrictions and regulations, limited collaboration, underdeveloped ecosystem, and security problems; the key attributes of MPS, and stakeholder and communication entities roles in MPS form different aspects. We discussed different security mechanisms involved in MPS. We also provide an analysis of the encryption technologies, authentication methods, and firewalls in MPS. All the papers suggest different techniques to provide different security aspects. However, the main point is that keeping in check the CIA triad, each payment should be made with authentication and encryption because the future of MPS depends on its security features.

REFERENCES

[1] S. F. Verkijika, "An affective response model for understanding the acceptance of mobile payment systems," *Electron. Commerce Res. Appl.*, vol. 39, Jan. 2020, Art. no. 100905.

[2] A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, "AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes," *J. Ambient Intell. Humanized Comput.*, pp. 1–14, Feb. 2020.

[3] S. Cimato, "Design of an authentication protocol for GSM Javacards," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Heidelberg, Germany: Springer, 2001, pp. 355–368.

[4] S. Kungpisdan, B. Srinivasan, and P. D. Le, "A practical framework for mobile set payment," in *Proc. Int. ESociety Conf.*, 2003, pp. 321–328.

[5] L. M. Marvel and C. G. Boncelet, "Authentication for low power systems," in *Proc. Commun. Netw.-Centric Oper., Creating Inf. Force (MILCOM)*, vol. 1, 2001, pp. 135–138.

[6] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," in *Proc. 2nd Int. Conf. Mobile Secure Services (MobiSecServ)*, Feb. 2016, pp. 1–5.

[7] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," *Trans. Emerg. Telecommun. Technol.*, p. e3935, Mar. 2020.

[8] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy G., R. Kaluri, G. Srivastava, and O. Jo, "KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.

[9] A. R. Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, and X. Liu, "Ensemble AdaBoost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Trans. Emerg. Telecommun. Technol.*, p. e4088, Aug. 2020.

[10] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, Apr. 2021.

[11] R. M. Mohammad and H. Y. AbuMansour, "An intelligent model for trustworthiness evaluation in semantic web applications," in *Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2017, pp. 362–367.

[12] D. Preuveneers, T. Heyman, Y. Berbers, and W. Joosen, "Feature-based variability management for scalable enterprise applications: Experiences with an e-payment case," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 5793–5802.

[13] E. Turban, J. Outland, D. King, J. K. Lee, T.-P. Liang, and D. C. Turban, "Mobile commerce and the Internet of Things," in *Electronic Commerce 2018*. Cham, Switzerland: Springer, 2018, pp. 205–248.

[14] M. Hubert, M. Blut, C. Brock, C. Backhaus, and T. Eberhardt, "Acceptance of smartphone-based mobile shopping: Mobile benefits, customer characteristics, perceived risks, and the impact of application context," *Psychol. Marketing*, vol. 34, no. 2, pp. 175–194, 2017.

[15] W. Stallings, *Cryptography and Network Security*. Hoboken, NJ, USA: Prentice-Hall, 2005, p. 592.

[16] *Securing the Future of Payments Together*. Accessed: May 14, 2020. [Online]. Available: https://www.brighttalk.com/webcast/17380/490469/securing-the-future-of-payments

[17] *The Home Depot Reports Findings in Payment Data Breach Investigation*, TH Depot, SANS, 2014.

[18] J. Téllez and S. Zeadally, *Mobile Payment Systems*. Cham, Switzerland: Springer, 2017.

[19] T. Dahlberg, J. Guo, and J. Ondrus, "A critical review of mobile payment research," *Electron. Commerce Res. Appl.*, vol. 14, no. 5, pp. 265–284, Sep./Oct. 2015.

[20] T. Dahlberg, N. Mallat, J. Ondrus, and A. Zmijewska, "Past, present and future of mobile payments research: A literature review," *Electron. Commerce Res. Appl.*, vol. 7, no. 2, pp. 165–181, Jun. 2008.

[21] J. Lee, M. H. Ryu, and D. Lee, "A study on the reciprocal relationship between user perception and retailer perception on platform-based mobile payment service," *J. Retailing Consum. Services*, vol. 48, pp. 7–15, May 2019.

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

[23] A. P. Thangamuthu, "A survey on various online payment and billing techniques," *Humanities*, vol. 7, no. 3, pp. 86–91, Jan. 2020.

[24] A. Saranya and R. Naresh, "Efficient mobile security for e health care application in cloud for secure payment using key distribution," *Neural Process. Lett.*, pp. 1–12, Mar. 2021.

[25] J. Wang and J.-Y. Lai, "Exploring innovation diffusion of two-sided mobile payment platforms: A system dynamics approach," *Technol. Forecasting Social Change*, vol. 157, Aug. 2020, Art. no. 120088.

[26] F. Liébana-Cabanillas, I. R. de Luna, and F. Montoro-Ríos, "Intention to use new mobile payment systems: A comparative analysis of SMS and NFC payments," *Econ. Res.-Ekonomska Istraživanja*, vol. 30, no. 1, pp. 892–910, Jan. 2017.

[27] M. Masihuddin, B. U. I. Khan, M. M. U. Islam Mattoo, and R. F. Olanrewaju, "A survey on e-payment systems: Elements, adoption, architecture, challenges and security concepts," *Indian J. Sci. Technol.*, vol. 10, no. 20, pp. 1–19, Jun. 2017.

[28] V. Kumar, K.-K. Lai, Y.-H. Chang, P. C. Bhatt, and F.-P. Su, "A structural analysis approach to identify technology innovation and evolution path: A case of m-payment technology ecosystem," *J. Knowl. Manage.*, vol. 25, no. 2, pp. 477–499, Mar. 2021.

[29] S. Solat, "Security of electronic payment systems: A comprehensive survey," 2017, *arXiv:1701.04556*. [Online]. Available: http://arxiv.org/abs/1701.04556

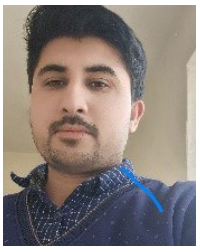
[30] M. Kim, S. Kim, and J. Kim, "Can mobile and biometric payments replace cards in the Korean offline payments market? Consumer preference analysis for payment systems using a discrete choice model," *Telematics Informat.*, vol. 38, pp. 46–58, May 2019.

[31] F. Liébana-Cabanillas, S. Molinillo, and M. Ruiz-Montañez, "To use or not to use, that is the question: Analysis of the determining factors for using NFC mobile payment systems in public transportation," *Technol. Forecasting Social Change*, vol. 139, pp. 266–276, Feb. 2019.

[32] I. R. de Luna, F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz-Leiva, "Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied," *Technol. Forecasting Social Change*, vol. 146, pp. 931–944, Sep. 2019.

[33] M. Sumathy and K. Vipin, "Digital payment systems: Perception and concerns among urban consumers," *IJAR*, vol. 3, no. 6, pp. 1118–1122, 2017.
[34] S. Fatonah, A. Yulandari, and F. Wibowo, "A review of e-payment system in e-commerce," *J. Phys., Conf. Ser.*, vol. 1140, Dec. 2018, Art. no. 012033.
[35] S. Evans and A. Pirchio, "An empirical examination of why mobile money schemes ignite in some developing countries but flounder in most," Univ. Chicago Coase-Sandor, Inst. Law Econ., Chicago, IL, USA, Res. Paper 723, 2015.
[36] P. van der Boor, P. Oliveira, and F. Veloso, "Users as innovators in developing countries: The global sources of innovation and diffusion in mobile banking services," *Res. Policy*, vol. 43, no. 9, pp. 1594–1607, Nov. 2014.
[37] S. Dodini, A. A. Lopez-Fernandini, E. A. Merry, and L. Thomas, "Consumers and mobile financial services 2016," Board Governors Federal Reserve Syst. (US), Washington, DC, USA, Tech. Rep. 1777, 2016.
[38] R. Duncombe, "Researching impact of mobile phones for development: Concepts, methods and lessons for practice," *Inf. Technol. Develop.*, vol. 17, no. 4, pp. 268–288, Oct. 2011.
[39] A. Dermish, C. Kneiding, P. Leishman, and I. Mas, "Branchless and mobile banking solutions for the poor: A survey of the literature," *Innov., Technol., Governance, Globalization*, vol. 6, no. 4, pp. 81–98, Oct. 2011.
[40] J. Liu, R. J. Kauffman, and D. Ma, "Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem," *Electron. Commerce Res. Appl.*, vol. 14, no. 5, pp. 372–391, Sep./Oct. 2015.
[41] N. Iman, "Is mobile payment still relevant in the fintech era?" *Electron. Commerce Res. Appl.*, vol. 30, pp. 72–82, Jul. 2018.
[42] A. A. Ozok and J. Wei, "An empirical comparison of consumer usability preferences in online shopping using stationary and mobile devices: Results from a college student population," *Electron. Commerce Res.*, vol. 10, no. 2, pp. 111–137, Jun. 2010.
[43] A. A. Shaikh and H. Karjaluoto, "Mobile banking adoption: A literature review," *Telematics Informat.*, vol. 32, no. 1, pp. 129–142, Feb. 2015.
[44] E. L. Slade, M. D. Williams, and Y. Dwivedi, "Extending UTAUT2 to explore consumer adoption of mobile payments," *UKAIS*, vol. 36, pp. 1–23, Mar. 2013.
[45] T. Oliveira, M. Thomas, G. Baptista, and F. Campos, "Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology," *Comput. Hum. Behav.*, vol. 61, pp. 404–414, Aug. 2016.
[46] V. Kumar, N. Nim, and A. Sharma, "Driving growth of mwallets in emerging markets: A retailer's perspective," *J. Acad. Marketing Sci.*, vol. 47, no. 4, pp. 747–769, 2019.
[47] R. Glavee-Geo, A. A. Shaikh, H. Karjaluoto, and R. E. Hinson, "Drivers and outcomes of consumer engagement," *Int. J. Bank Marketing*, vol. 38, no. 1, pp. 1–20, Jul. 2019.
[48] T. Apanasevic, J. Markendahl, and N. Arvidsson, "Stakeholders ' expectations of mobile payment in retail: Lessons from Sweden," *Int. J. Bank Marketing*, vol. 34, no. 1, pp. 37–61, Feb. 2016.
[49] J. T. Isaac and Z. Sherali, "Secure mobile payment systems," *IT Prof.*, vol. 16, no. 3, pp. 36–43, May/Jun. 2014.
[50] 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.
[51] P. Chaudhury, S. Dhang, M. Roy, S. Deb, J. Saha, A. Mallik, S. Bal, S. Roy, M. K. Sarkar, S. Kumar, and R. Das, "ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm," in *Proc. 8th Annu. Ind. Autom. Electromech. Eng. Conf. (IEMECON)*, Aug. 2017, pp. 332–337.
[52] J. Zhang, "A study on application of digital signature technology," in *Proc. Int. Conf. Netw. Digit. Soc.*, vol. 1, 2010, pp. 498–501.
[53] S. F. Al-Janabi and A. K. Obaid, "Development of certificate authority services for web applications," in *Proc. Int. Conf. Future Commun. Netw.*, Apr. 2012, pp. 135–140.
[54] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decis. Support Syst.*, vol. 106, pp. 1–14, Feb. 2018.
[55] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. Cham, Switzerland: Springer, 2007.
[56] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in eBanking and the effects of experience," *Interacting Comput.*, vol. 22, no. 3, pp. 153–164, May 2010.
[57] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Secur.*, vol. 39, pp. 127–136, Nov. 2013.
[58] S. Byun and S.-E. Byun, "Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters," *Behav. Inf. Technol.*, vol. 32, no. 3, pp. 217–230, Mar. 2013.
[59] I. M. Alsaadi, "Physiological biometric authentication systems, advantages, disadvantages and future development: A review," *Int. J. Sci. Technol. Res.*, vol. 4, no. 12, pp. 285–289, 2015.
[60] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1998–2026, 3rd Quart., 2016.
[61] M. Rouse. (2017). *Single-Factor Authentication (SFA)*. [Online]. Available: https://searchsecurity.techtarget.com/
[62] A. Rahav. (2018). *The Secret Security Wiki*. [Online]. Available: https://doubleoctopus.com/security-wiki/authentication/single-factor-authentication/
[63] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, Jan. 2018.
[64] C. Hamilton and A. Olmstead, "Database multi-factor authentication via pluggable authentication modules," in *Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2017, pp. 367–368.
[65] K. K. Lakshmi, H. Gupta, and J. Ranjan, "USSD—Architecture analysis, security threats, issues and enhancements," in *Proc. Int. Conf. INFOCOM Technol. Unmanned Syst. (Trends Future Directions) (ICTUS)*, Dec. 2017, pp. 798–802.
[66] S. Castle, F. Pervaiz, G. Weld, F. Roesner, and R. Anderson, "Let's talk money: Evaluating the security challenges of mobile money in the developing world," in *Proc. 7th Annu. Symp. Comput. Develop.*, Nov. 2016, pp. 1–10.
[67] B. Reaves, J. Bowers, N. Scaife, A. Bates, A. Bhartiya, P. Traynor, and K. R. B. Butler, "Mo (bile) money, mo (bile) problems: Analysis of branchless banking applications," *ACM Trans. Privacy Secur.*, vol. 20, no. 3, pp. 1–31, Aug. 2017.
[68] R. Mahajan, J. Saran, and A. Rajagopalan, "Mitigating emerging fraud risks in the mobile money industry," Deloitte, Mumbai, India, Tech. Rep., 2015.
[69] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019.
[70] M. W. Buku and R. Mazer, "Fraud in mobile financial services: Protecting consumers, providers, and the system," World Bank, Washington, DC, USA, Tech. Rep., 2017.
[71] S. Lonie, "Fraud risk management for mobile money: An overview. 2017," GSMA, London, U.K., Tech. Rep., 2017.
[72] P. Sharma, "A contemplate on multifactor authentication," in *Proc. 6th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2019, pp. 824–827.
[73] A. Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar, and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *J. Inf. Secur. Appl.*, vol. 51, Apr. 2020, Art. no. 102443.
[74] L. Katusiime, "Mobile money use: The impact of macroeconomic policy and regulation," *Economies*, vol. 9, no. 2, p. 51, Apr. 2021.
[75] K. McKee, M. Kaffenberger, and J. M. Zimmerman, "Doing digital finance right: The case for stronger mitigation of customer risks," *Focus Note*, vol. 103, 2015.
[76] G. Ali, M. A. Dida, and A. Elikana Sam, "Evaluation of key security issues associated with mobile money systems in Uganda," *Information*, vol. 11, no. 6, p. 309, Jun. 2020.
[77] R. Gwahula, "Risks and barriers associated with mobile money transactions in Tanzania," Macrothink Inst., Las Vegas, NV, USA, Tech. Rep., 2016.
[78] 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.
[79] D. Kunda and M. Chishimba, "A survey of Android mobile phone authentication schemes," *Mobile Netw. Appl.*, pp. 1–9, Aug. 2018.
[80] F. S. G. Talom and R. K. Tengeh, "The impact of mobile money on the financial performance of the SMEs in Douala, Cameroon," *Sustainability*, vol. 12, no. 1, p. 183, Dec. 2019.

[81] B. W. Nyamtiga, A. Sam, and L. S. Laizer, "Enhanced security model for mobile banking systems in Tanzania," *Intl. Jour. Tech. Enhancements Emerg. Eng. Res.*, vol. 1, no. 4, pp. 4–20, 2013.
[82] W. Ahmed, F. Shahzad, A. R. Javed, F. Iqbal, and L. Ali, "WhatsApp network forensics: Discovering the IP addresses of suspects," in *Proc. 11th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Apr. 2021, pp. 1–7.
[83] A. Chowdhury, "Recent cyber security attacks and their mitigation approaches—An overview," in *Proc. Int. Conf. Appl. Techn. Inf. Secur.* Singapore: Springer, 2016, pp. 54–65.
[84] M. S. Sadekin, "Security of e-banking in Bangladesh," *J. Finance Accounting*, vol. 4, no. 1, p. 1, 2016.
[85] A. 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.
[86] N. Shaw, "The mediating influence of trust in the adoption of the mobile wallet," *J. Retailing Consum. Services*, vol. 21, no. 4, pp. 449–459, Jul. 2014.
[87] N. Kshetri, "Cybercrime and cybersecurity in Africa," *J. Global Inf. Technol. Manage.*, vol. 22, no. 2, pp. 77–81, 2019.
[88] L. Tamazirt, F. Alilat, and N. Agoulmine, "NFC-based ubiquitous monitoring system for e-industry," in *Proc. 3rd Int. Conf. Mobile Secure Services (MobiSecServ)*, Feb. 2017, pp. 1–4.
[89] A. Bhatta and A. K. Mishra, "GSM-based commsense system to measure and estimate environmental changes," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 2, pp. 54–67, Feb. 2017.
[90] Y.-C. Tsao, Q. Zhang, and Q. Zeng, "Supply chain network design considering RFID adoption," *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 2, pp. 977–983, Apr. 2016.
[91] S. Dix, I. Phau, K. Jamieson, and A. S. Shimul, "Investigating the drivers of consumer acceptance and response of SMS advertising," *J. Promotion Manage.*, vol. 23, no. 1, pp. 62–79, Jan. 2017.
[92] S. Mukherjee and S. Mondal, "A scheme for qr code based smart door locks security system using an arm computer," in *Proc. 1st Int. Conf. Intell. Comput. Commun.* Singapore: Springer, 2017, pp. 613–621.
[93] S. S. Hassan, S. D. Bibon, M. S. Hossain, and M. Atiquzzaman, "Security threats in Bluetooth technology," *Comput. Secur.*, vol. 74, pp. 308–322, May 2018.
[94] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from RSA without pairings," *Int. J. Netw. Secur.*, vol. 19, no. 2, pp. 229–235, 2017.
[95] J. M. Kizza, "Security in wireless networks and devices," in *Guide to Computer Network Security*. Cham, Switzerland: Springer, 2017, pp. 397–427.
[96] M. A. Qadeer, N. Akhtar, S. Govil, and A. Varshney, "A novel scheme for mobile payment using RFID-enabled smart SIMcard," in *Proc. Int. Conf. Future Comput. Commun.*, Apr. 2009, pp. 339–343.
[97] S. S. Manvi, L. B. Bhajantri, and M. A. Vijayakumar, "Secure mobile payment system in wireless environment," in *Proc. Int. Conf. Future Comput. Commun.*, Apr. 2009, pp. 31–35.
[98] J. Liu, J. Liao, and X. Zhu, "A system model and protocol for mobile payment," in *Proc. IEEE Int. Conf. e-Bus. Eng. (ICEBE)*, Oct. 2005, pp. 638–641.
[99] X. Zheng and D. Chen, "Study of mobile payments system," in *Proc. IEEE Int. Conf. E-Commerce (CEC)*, Jun. 2003, pp. 24–27.
[100] W. Chen, G. P. Hancke, K. E. Mayes, Y. Lien, and J.-H. Chiu, "NFC mobile transactions and authentication based on GSM network," in *Proc. 2nd Int. Workshop Near Field Commun.*, 2010, pp. 83–89.
[101] M. Al-Tamimi and A. Al-Haj, "Online security protocol for NFC mobile payment applications," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, May 2017, pp. 827–832.
[102] S. Nseir, N. Hirzallah, and M. Aqel, "A secure mobile payment system using QR code," in *Proc. 5th Int. Conf. Comput. Sci. Inf. Technol.*, Mar. 2013, pp. 111–114.
[103] S.-W. Chen and R. Tso, "NFC-based mobile payment protocol with user anonymity," in *Proc. 11th Asia Joint Conf. Inf. Secur. (AsiaJCIS)*, Aug. 2016, pp. 24–30.
[104] A. T. Purnomo, Y. S. Gondokaryono, and C.-S. Kim, "Mutual authentication in securing mobile payment system using encrypted QR code based on public key infrastructure," in *Proc. 6th Int. Conf. Syst. Eng. Technol. (ICSET)*, Oct. 2016, pp. 194–198.
[105] T. Ma, H. Zhang, J. Qian, X. Hu, and Y. Tian, "The design and implementation of an innovative mobile payment system based on QR bar code," in *Proc. Int. Conf. Netw. Inf. Syst. Comput.*, Jan. 2015, pp. 435–440.
[106] Y. Rui-Xia, "Design of secure mobile payment system based on IBC," in *Proc. 10th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2015, pp. 422–425.
[107] H. Harb, H. Farahat, and M. Ezz, "SecureSMSPay: Secure SMS mobile payment model," in *Proc. 2nd Int. Conf. Anti-Counterfeiting, Secur. Identificat.*, 2008, pp. 11–17.
[108] M. H. Firoz and Z. Ahmed, "Defensive protocol to ensure safe mobile financial transaction in current context," in *Proc. 3rd Asian Conf. Defence Technol. (ACDT)*, Jan. 2017, pp. 54–58.
[109] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, "U2F based secure mutual authentication protocol for mobile payment," in *Proc. ACM Turing 50th Celebration Conf. China (ACM TUR-C)*, 2017, pp. 1–6.
[110] F. Shahzad, W. Iqbal, and F. S. Bokhari, "On the use of CryptDB for securing electronic health data in the cloud: A performance study," in *Proc. 17th Int. Conf. e-Health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 120–125.
[111] C. Ruan, F. Xiao, and J. Luo, "Desgn and implementation of mobile payment system for intelligent travel," in *Proc. IEEE 3rd Int. Conf. Cloud Comput. Intell. Syst.*, Nov. 2014, pp. 547–552.
[112] B. Singh and K. S. Jasmine, "Comparative study on various methods and types of mobile payment system," in *Proc. Int. Conf. Adv. Mobile Netw., Commun. Appl.*, Aug. 2012, pp. 143–148.
[113] S. Bojjagani and V. N. Sastry, "A secure end-to-end SMS-based mobile banking protocol," *Int. J. Commun. Syst.*, vol. 30, no. 15, p. e3302, Oct. 2017.
[114] J. Kang and D. Nyang, "A privacy-preserving mobile payment system for mass transit," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 8, pp. 2192–2205, Aug. 2017.
[115] W. A. Khan, Y. Saleem, G. A. Shah, and A. Farooq, "Modified mobile transaction authentication number system for 2-layer security," in *Proc. Int. Conf. Intell. Syst. Eng. (ICISE)*, Jan. 2016, pp. 89–93.
[116] J. N. Luo, M. H. Yang, and S.-Y. Huang, "An unlinkable anonymous payment scheme based on near field communication," *Comput. Electr. Eng.*, vol. 49, pp. 198–206, Jan. 2016.
[117] G. Platform, "The trusted execution environment: Delivering enhanced security at a lower cost to the mobile market," Global Platform, Malaysia, White Paper, Feb. 2011.
[118] V. Sureshkumar, R. Anitha, N. Rajamanickam, and R. Amin, "A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity," *Comput. Electr. Eng.*, vol. 57, pp. 223–240, Jan. 2017.
[119] S. Bojjagani and V. N. Sastry, "SSMBP: A secure SMS-based mobile banking protocol with formal verification," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 252–259.
[120] D. L. Lavanya, R. Ramaprabha, B. Thangapandian, and K. Gunaseelan, "Novel privacy preserving authentication scheme based on physical layer signatures for mobile payments," *Social Netw. Comput. Sci.*, vol. 2, no. 2, pp. 1–11, Apr. 2021.
[121] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient iot devices using blockchain," in *Proc. Int. Conf. Smart City Informatization*. Singapore: Springer, 2019, pp. 334–348.



WAQAS AHMED is currently pursuing the Ph.D. degree with the Department of Cyber Security, Air University, Islamabad, Pakistan. His research interests include machine learning, wireless sensor networks, mobile computing, and security issues in mobile cloud computing.

AAMIR RASOOL is currently pursuing the M.S. degree with Air University, Islamabad. His research interests include machine learning, natural language processing, and computer vision.

ABDUL REHMAN JAVED (Member, IEEE) received the master's degree in computer science from the National University of Computer and Emerging Sciences, Islamabad, Pakistan. He worked with the National Cybercrimes and Forensics Laboratory, Air University, Islamabad, Pakistan. He is currently a Lecturer with the Department of Cyber Security, Air University. He is also a Cybersecurity Researcher and a Practitioner with industry and academic experience. He has reviewed over 150 scientific research articles for various well-known journals including, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Computer and Electrical Engineering* (Elsevier), *Sustainable Cities and Society* (Elsevier), *Journal of Information Security and Applications* (Elsevier), *IEEE Internet of Things Magazine*, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, *Transactions on Internet Technology* (ACM), *Telecommunication Systems* (Springer), IEEE ACCESS, and *International Journal of Ad Hoc and Ubiquitous Computing* (Inderscience). He has authored over 50 peer-reviewed research articles. He is supervising/co-supervising several graduate (B.S. and M.S.) students on topics related to health informatics, cybersecurity, mobile computing, and digital forensics. His research interests include mobile and ubiquitous computing, data analysis, knowledge discovery, data mining, natural language processing, smart homes, and their applications in human activity analysis, human motion analysis, and e-health. He aims to contribute to interdisciplinary research of computer science and human-related disciplines. He is an ACM Member. He is a TPC Member of CID2021 (Fourth International Workshop on Cybercrime Investigation and Digital Forensics-CID2021) and the 44th International Conference on Telecommunications and Signal Processing. He has served as a Moderator for the 1st IEEE International Conference on Cyber Warfare and Security (ICCWS).

NEERAJ KUMAR (Senior Member, IEEE) received the Ph.D. degree in CSE from SMVD University, Katra, Jammu and Kashmir, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. Since 2014, he has been working as an Associate Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala, Punjab, India. He is a Visiting Research Fellow with Coventry University. He is an internationally renowned researcher in the areas of VANET & CPS smart grid & the IoT mobile cloud computing & big data and cryptography. He has published more than 150 technical research articles in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, and Taylor & Francis. His paper has been published in some of the high-impact factors journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON POWER SYSTEMS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON SMART GRID, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, IEEE ACCESS, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE SYSTEMS JOURNAL, IEEE INTERNET OF THINGS JOURNAL, *IEEE Wireless Communication Magazine*, *IEEE Vehicular Technology Magazine*, *IEEE Communication Magazine*, and *IEEE Networks Magazine*. Apart from the journals conferences, he has also published papers in some of the core conferences of his area of specialization such as IEEE Globecom, IEEE ICC, IEEE Greencom, and IEEE CSCWD. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. His research is supported by funding from TCS, CSIT, UGC and UGC in the area of smart grid, energy management, VANETs, and cloud computing. He is a member of the Cyber-Physical Systems and Security (CPSS) Research Group. He has research funding from DST, CSIR, UGC, and TCS. He has total research funding from these agencies of more than two crores under different schemes from the GOI. Recently, he has also got international research projects under DST-research initiative. He has H-index of 26 (according to Google scholar, March 2017) with 2500 citations to his credit. He is an Editorial Board Member of *International Journal of Communication Systems* (Wiley), *Security and Communication* (John Wiley), and *Journal of Networks and Computer Applications* (Elsevier). He has visited many countries mainly for the academic purposes. He has many research collaborations with premier institutions in India and different universities across the globe. He has been engaged in different academic activities inside and outside the institute. He has supervised five Ph.D. students and five are currently pursuing their thesis. He has also supervised more than 20 M.E./M.Tech. thesis.

THIPPA REDDY GADEKALLU received the B.Tech. degree in CSE from Nagarjuna University, India, the M.Tech. degree in CSE from Anna University, Chennai, Tamil Nadu, and the Ph.D. degree from VIT, Vellore, Tamil Nadu, India. He is currently working as an Associate Professor with the School of Information Technology and Engineering, VIT. He has more than 14 years of experience in teaching. He has published more than 50 international/national publications. His research interests include machine learning, the Internet of Things, deep neural networks, blockchain, and computer vision.

ZUNERA JALIL (Member, IEEE) received the master's degree in computer science with a scholarship from the Higher Education Commission of Pakistan, in 2007, and the Ph.D. degree in computer science with specialization in information security from the FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2010. She has served as a full-time Faculty Member with International Islamic University, Islamabad, Iqra University, Islamabad, and Saudi Electronic University, Riyadh, Saudi Arabia. She is currently an Assistant Professor with the Department of Cyber Security, Faculty of Computing and Artificial Intelligence, Air University, Islamabad. She is also a Senior Researcher with the National Cybercrimes and Forensics Laboratory, National Center for Cyber Security, Islamabad. Her research interests include computer forensics, machine learning, criminal profiling, software watermarking, intelligent systems, and data privacy protection.

NATALIA KRYVINSKA received the Ph.D. degree in electrical and IT engineering from Vienna University of Technology, Austria, and a Docent title (Habilitation) in management information systems from the Comenius University in Bratislava, Slovakia. She got her Professor title and was appointed for the professorship by the President of Slovak Republic. She worked as a University Lecturer and a Senior Researcher with the eBusiness Department, University of Vienna's School of Business Economics and Statistics. She is currently a Full Professor and the Head of the Information Systems Department, Faculty of Management, Comenius University in Bratislava, Slovakia. Her research interests include complex service systems engineering, service analytics, and applied mathematics.