International Journal of Communication Networks and Information Security
2024, 16(1), 5756
ISSN: 2073-607X,2076-0930
https://ijcnis.org/

Research Article

Improve Privacy-Preserving for User Identity: Possibilities, Challenges, and Future Directions

Shahad Alotaibi [1], Suliman Aladhadh [2*]

[12] Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia
*Corresponding Author: s.aladhadh@qu.edu.sa

Citation: S. Alotaibi and S. Aladhadh, "Improve Privacy-Preserving for User Identity: Possibilities, Challenges, and Future Directions," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 16, no. 1, pp. 271-282 ,Jan.2024.

ARTICLE INFO

Received: 15 November 2023
Accepted: 6 April 2024

ABSTRACT

Electronic payment via mobile devices has become the modern way of payment. While facilitating and speeding up many payment processes, this method also brings about certain crucial problems related to electronic payment where the users fear putting the security of their bank accounts and personal information at risk in electronic payment operations. Electronic payment services do not fully secure personal accounts and may be subjected to violations. Yet compared to traditional offline mode payment channels, mobile payments are transforming the supply chain of businesses and sectors and are crucial to the rapid expansion of online markets. The kind of mobile payment channel utilized, the security infrastructure that accompanies it, the stakeholders engaged, and the m-business models chosen all have a role in the success of an e-business. However, concerns about preserving the identity and privacy of users, referred to by users as sensitive information, should not be dealt with via the Internet. In this study, we describe the most recent research in this field and give a thorough literature review of mobile payment.

Keywords: Security, Mobile Payment, Encryption, User Identity, Data Privacy, ECC.

INTRODUCTION

In recent years, an increase in the use of mobile phones has been observed; this has led to a rise in the percentage of electronic payments, i.e., "mobile payment" [1]. For example, Apple Pay, Apple's first mobile payment service, was launched in 2014, and it was quickly followed by Samsung and Android payment systems. Mobile payment is the term used to describe payment services carried out via a mobile device.

Rather than using traditional methods such as credit cards or cash, users can pay for numerous services and goods using their mobile phones. By 2022, the global transaction value for mobile payments was expected to reach $14 trillion [2].

Perceived security and privacy hazards, as well as the disadvantages of relying on a mobile phone and a lack of perceived proportional advantages over alternative payment choices, are significant roadblocks to adoption [3]. The massive growth of smart mobile devices has attracted numerous payment apps which involve more sophisticated interactions between multiple participants compared to traditional payments. Therefore, such payment apps are error-prone and could be exploited easily, leading to serious financial deceptions.

We have entered an era that is focused on the implementation of mobile payment operations, due to the ease of this process which obtains the product faster than before. Thus, mobile phones have become a widespread and essential commodity for payment use.

However, while electronic and online payment systems have seen considerable growth, mobile payments have fallen short of expectations. By considering the various problems related to the structure of the user's approval of the electronic payment process, there are many suggestions for implementing a secure payment

process to preserve the privacy of users [4], [5]. It is a well-known fact that after the development of mobile phone technologies, all operations require use of the phone; the most important operation is electronic payment.

Following an analysis of the data gathered from the systematic Survey Research (SLR) for mobile payment research, discussions that follow each phase are provided. This paper has two research questions:

What methods are relied upon to analyze the most important factors affecting mobile payment adoption?

How can mobile payment privacy be maintained using the most important modern methodology?

The following sections are presented as follows:

The first sections of the paper contribute to the analysis and determination of the development of electronic payment processes, specifically in the use of quick response codes in mobile payment as well as improving the model of preserving user privacy and banking information used in payment operations, especially for payments to stores. Section 1 discusses the motivation of the research, section 2 focuses on the contribution to research work, section 3 reviews previous literature, section 4 describes the methodology and presents the expected results, and lastly, section 5 provides the results and evaluates the performance of the proposed methodology.

OVERVIEW OF GROWTH OF MOBILE PAYMENT SYSTEMS (MPSs)

One way to boost revenue growth in the financial and commercial sectors is through mobile payments. The industry's financial growth was expected to increase by approximately 38% between 2010 and 2020. This is a result of the anticipated growth in both traditional banking and mobile payments. According to Figure 1, both the number of mobile payment users and the number of mobile payment transactions are growing at impressive rates. In many parts of the world, the number of mobile payment users is growing (as of 2016, there were (64 + 90.7 + 163.6 + 6 + 101.3 + 22.3 = 447.9$) million transactions). Additionally, global mobile payment spending reached $1.3 trillion in 2017.

Mobile payment, according to Juniper Research [6]:

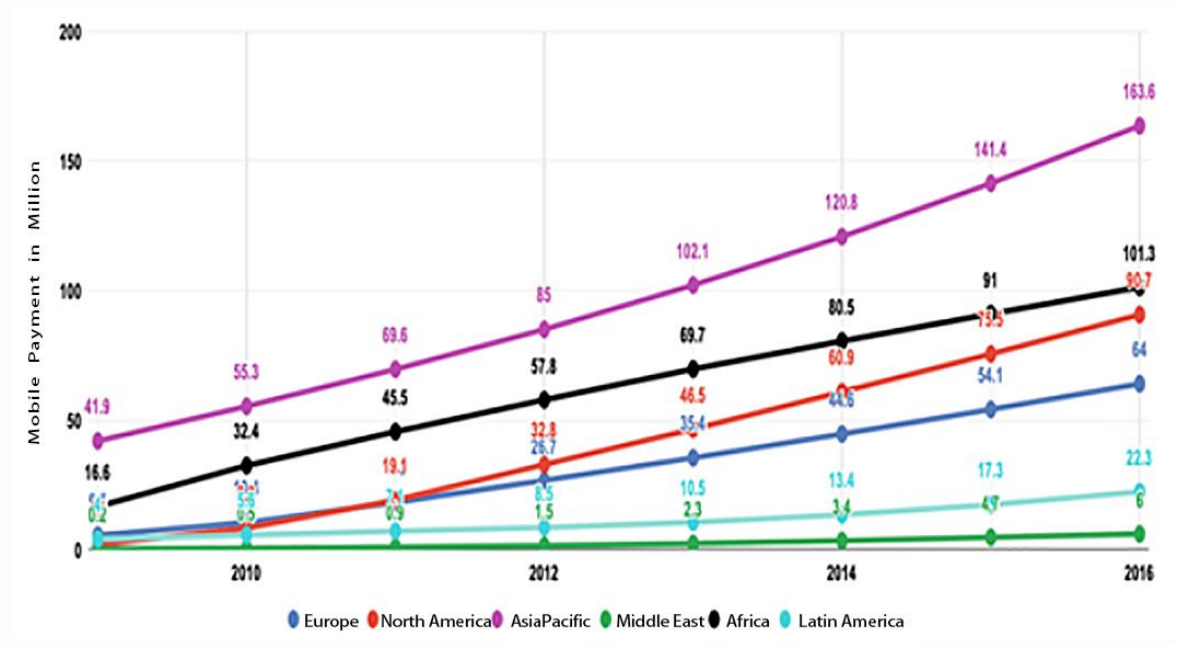

Figure 1. Mobile Payment Customers from 2009 to 2016 by Region (in Millions) [6].

According to a recent study by Juniper Research [7], the number of mobile payment transactions would increase by 92% from 26 billion in 2021 to 49 billion in 2023. By 2023, the volume of mobile contactless transactions would have greatly surpassed that of contactless card transactions owing to the two-times-faster growth of mobile contactless transactions. The report recognized mobile contactless payments' improved security and expansion of cross-channel payment capabilities as two of its main development drivers.

ANALYSIS OF SYSTEMATIC LITERATURE REVIEW

This section involves an overview of the literature most closely related to the currently proposed research that discusses the adoption of using mobile payment technology.

Intention and Adaptation of Using a Mobile-Payment System

This section describes the operative that impacts individual agreement and adoption of using new technology. Emerging technologies provide a growing level of social interaction and new approaches to understanding modern technologies because social aspects affect the extent to which mobile payment technologies are adopted.

Mobile Technology Acceptance Model (MTAM)

Developed by Davis in 1989, [7] is one of the most important models of technology assent, identifying two primary factors that influence an individual's aim to use new technology. There may be a difference in the percentage of disparity in the acceptance of technology, especially in the advancement of technologies that support mobile financial payments. It is clear that there are two categories. Young adults may accept the rise of mobile payment technologies as inevitable and aspire to experience these technologies. In contrast, older adults may believe that they are time-wasting techniques that have no reliable security; therefore, they do not want to try them. There may be several reasons that prevent maybe they have from seeing this development in mobile payment technologies.

Yan et al. [1] focused on the intention to pay by quick response code through the mobile phone technology approval model, and the results of the theory focus on the extent to which users accept this type of technology. The researchers' findings identified the extent to which the users accepted the deployment of electronic payment using mobile phones, the convenience it offers in retail sales, and the flexibility and ease of this type of payment in accelerating the payment process. Also, an effect between PTC has been discovered to significantly influence the usefulness of m-payment, and MEOU has a positive relationship with BI to adopt QR code in m-payment. The study was conducted during the COVID-19 period during which people completely shifted from cash to card payments to avoid and limit the spread of the disease. From this study, it is evident that mobile payment will have significant importance in the future.

Research by De Luna et al. [2] evaluates the elements that influence consumers' acceptance of short message service (SMS), near field communication (NFC), and quick response (QR) mobile payment systems, as well as the main factors that influence their uptake as payment methods [8].

The study's findings and innovation come from the formulation of different behaviors based on how users use each of the proposed payment options. First, it presents a comparative examination of the three most common mobile payment methods used by businesses today. Second, the research was conducted in Spain, where all three technologies are still in their early stages of adoption, and so the findings are applicable. The main goal of this study is to examine customer acceptance of SMS, NFC, and QR mobile payment systems using a behavioral model and find the elements that influence it. In this sense, the models have variances of 0.317, 0.654, and 0.574 for intention to use, respectively. To accomplish this, the researchers looked at aspects related to the technology acceptance model in several contexts involving payment systems, including Internet banking, mobile banking, and mobile payments.

According to Bojjagani et al. [6], one of the fastest-growing mobile services today is mobile payments, and it has been discovered that the widespread usage of cell phones for online shopping, bill payment, and utility payments is contributing to the spectacular expansion of online markets. Compared to traditional offline payment methods and online e-channels such as ATM, e-check, and e-card transactions, mobile payments are becoming more and more popular. The authors present a systematic literature review (SLR) on mobile payments in this study, which compiles the most recent studies made in this area from 2000 to 2020.

Based on the investigation, they have demonstrated significant barriers as well as trends, patterns, new technologies, inventions, and gaps in the body of existing research. The researchers assert that the developers of mobile payment applications may not take secure coding practices into account in order to achieve security features like confidentiality, data integrity, non-repudiation, and authorization after considering the findings of earlier research and the gap in electronic payment processes.

Mobile Payment Adoption of User

This section reviews qualitative studies by classifying the intention to adopt mobile payment and presenting theories about the security concerns that led to the reduction of mobile payment adoption rates which may harm the development of technologies in electronic payment processes. We review some theories below.

Ganesan et al. [9] identified the most significant risks and challenges faced by smartphone users in electronic payment operations. The researchers' proposed work analyzes the information security risks in mobile payment technology. The proposed model is derived by tracking risks, analyzing interviews with experts, and assessing the likelihood of potential risks in the electronic payment process. The researchers conducted interviews with eight people from different disciplines and ranks in information security and data management. The researchers used the AHP model to analyze potential risks with experts. The results of the model determined the levels of risk where the first ranks were loss of confidential data (42%), leakage of personal data (41%), and financial losses (28%) with the highest average supported by experts in their analysis.

De et al. [2] focused on the new experience with the payment process using the QR code, where a simple user interface is designed with fewer details in order to provide the service to users with limited knowledge of using modern devices and electronic payment processes. The researchers conducted interviews with users with limited knowledge to find out the difficulties they face in the M-payment process. Accordingly, the user interface was designed for them as well as for those who are knowledgeable, but in a clearer way. The user interface proposed earlier by researchers was difficult because it contained many details in the entry. As well, the process of verifying the identity of the user was weak.

Lian et al. [3] analyzed the dimensions of trust in the use of electronic payment services in Taiwan. Following an analysis of studies on the perspective of trust, it became clear that there is a gap between trust in the use of electronic payments and its acceptance. The researchers analyzed these problems using a model as well as the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) by putting forth some theories and a questionnaire to collect the required data. SmartPLS was employed to validate the proposed model and hypotheses.

Findings: Upon analyzing responses from 683 participants, the results revealed that the significant antecedents of overall trust include trust in mobile payment service providers, mobile devices, and merchants (R2=75%). Furthermore, overall trust has significant effects on performance, efforts, and expectations with regard to mobile payment. Finally, the determinants of continuous usage intention include overall trust, performance expectancy, effort expectancy, facilitating conditions, hedonic motivation, habit, and perceived value (R2=85%). Originality: "Trust" in mobile payment is a common concern in developing mobile payment methods.

Pešterac et al. [10] stated that in today's digital world, maintaining data privacy is a major challenge. The following quandary arises from smart gadgets or security. In other words, how much can customers trust a service provider when fraud is a possibility? Electronic payment systems are especially vulnerable to this type of vulnerability. Although all payment systems have security vulnerabilities, electronic payment systems in the IoT environment have increased the potential for user data exploitation. The use of non-standardized technology raises the vulnerability of the entire system, increasing the risk of fraud. The massive volume of data that passes through payment systems can provide insight into customer spending habits as well as a potential tool for detecting and preventing fraud. The digital world is gradually eliminating the boundaries of data privacy.

In Table 1, a review of the classification of previous research has been performed by quantitative and qualitative research regarding the adoption of mobile payment.

Table 1. The Classification of Security Factors Affecting Mobile Payment

Type of Research	References	Empirical Qualitative	Empirical Quantitative	Quantitative Conceptual Speculative Commentary
Mobile Technology Acceptance Model	[1], [7]-[9]	0	4	4
Mobile Payment Adoption Theories	[2], [3], [10], [11],[12], [13]	4	2	2

Mobile Payment in Privacy Preservation

This section examines various security implementations and issues that exist in solutions that carry out such transactions using mobile payments as an organizational framework.

Distribution of Articles Based on Security and Privacy Protocols in Mobile Payments

This section mainly focuses on various approaches to security and privacy. Since mobile payments lack security and transaction properties, this will severely restrict their use in commerce applications. In this stage, the research areas are categorized according to 1) Protocol approaches for safe mobile payment exchanges; and 2)

Strategies for PKI/WPKI, the secure electronic transaction (SET) protocol, and Near Field Communication (NFC)-based mobile payments.

Regarding the NFC payment model in smartphones and bank cards, El Madhoun et al. [11] noted that the payment transaction can be executed instantly without the need for physical contact, PIN code entry, or signature. However, the researchers pointed out a few security shortcomings in the payment process: the authentication of the payment terminal to the customer's payment device, and the personal banking data of customers. The researchers proposed a model for a security protocol in the implementation of the payment transaction via mobile phones, NFC technology, smartphones, and payment terminals, which gives a security solution for EMV by adding a new security layer to ensure mutual authentication and non-repudiation, and to ensure that customers' bank data are encrypted. Authentication is still a problem in other protocols in ensuring the payment process between the worker and the customer in the provision of services. Figure 2 explains the procedure of NFC security protocol.

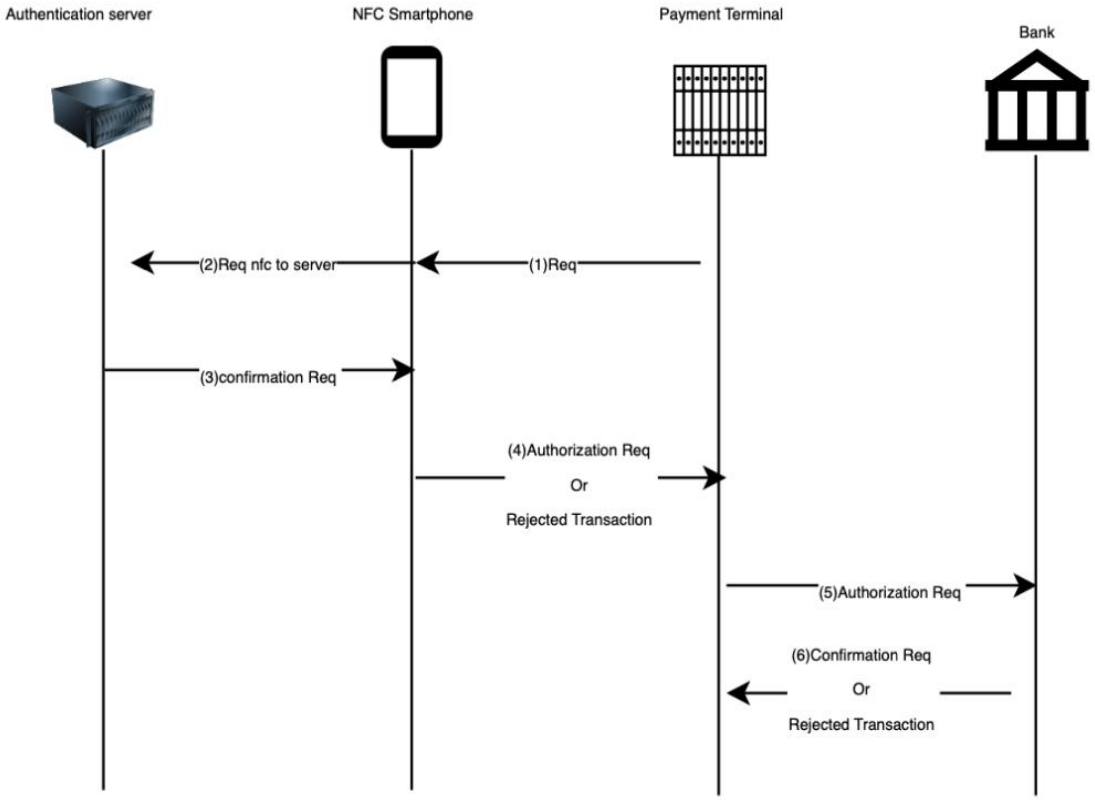

Figure 2. Proposed Near Field Communication (NFC) Security Protocol [8]

Sung et al. [12] note that the cryptocurrency wallet is vulnerable to key theft when connected to a transaction network. Despite the fact that it cannot be tracked, blockchain should exchange data with other blockchains. This study offers a crucial protocol architecture to protect Bitcoin transactions for user privacy in order to handle the problem of decentralized exchange and connect with blockchain application data. The Federated Byzantine Agreement (FBA) for key-exchange agreements between users is included in the key protocol along with a session key for a blockchain data structure. The values for key cluster-mode, test session key mode, and original session key mode were calculated using the F-measure model. Creating and growing safe extended networks is encouraged because the proposed protocol may have flaws and there are still concerns about maintaining trust in digital currency.

Yang et al. [13] pointed out that mobile phone applications in electronic payment have loaded a lot of security flaws that may hinder payment through the mobile phone. The researchers also recommended analyzing the applications and obtaining a set of statistics and potential risks, as unsecured payment in the morning poses a major threat to the mobile ecosystem as more and more electronic transactions are transmitted. The researchers suggested the analysis of embedded applications using SDK packages for in-app payment from third parties at risk. As well, they also detected seven cases of security rule violation on both Android and iOS platforms. It is necessary to try to enhance the security of these applications which have become a large part of our lives. With the development of technologies, mobile payment has become a central point of payment.

Secure Mutual Authentication Protocol and Privacy-Preserving Protocols in Mobile Payment

This section explains the most well-known mobile payment protocols/frameworks and the most important features that help protect sensitive/private data. This section also discusses the multi-perspective framework for mobile payment systems.

Zamanian et al. [14] focused on a wireless setting. Mobile commerce allows transactions to be completed via mobile devices. Several mobile payment methods have already been created in an attempt to meet users' security needs. Fair-exchange requirements have received little attention in mobile payment protocols thus far, despite the fact that it is a critical aspect in the eyes of users. Clients must pay for the product before it is delivered in most mobile payment systems. This unfair position is remedied in this work by providing a mobile payment protocol that meets both security and fair-exchange requirements. The APSWPP protocol is the foundation for this protocol. In this protocol, the client receives a committed product before paying for it, and after paying for it, it can obtain the committed product's secret. Some stages have been added to the core phases of this protocol to fully serve fair-exchange. The AVISPA tool verifies the security of our proposed protocol.

Ahamad et al. [15] noted that, as previously mentioned, mobile contactless payment (MCP) is the upcoming technology for mobile wallets and payments.

End-to-end communication, data security, or client anonymity are not promises made by the available solutions in this field. A near-field communication (NFC)-based, secure and privacy-preserving mobile commerce (SPPMC) architecture for proximity payments is presented as a solution to these flaws. It uses traceable anonymous certificates (TAC) to preserve the client's privacy. Using a grid of secure elements (GSE), banking servers are protected. Computation and communication are inexpensive. SPPMC offers complete defense and is resistant to all known assaults, including those utilizing multiple protocols.

For this reason, the researchers proposed this model in the context of maintaining bank accounts since they hold all personal and bank accounts of the beneficiary while safeguarding the privacy of consumers by paying via mobile phone for contactless payment.

According to Fan et al. [16], over the past ten years, as financial technology has gained popularity, the e-commerce sector has experienced rapid expansion. This is especially true for mobile payments, which are becoming more widespread. In this paper, the authors propose a secure mutual authentication protocol (SMAP) for mobile payments that is based on the universal second factor (U2F) protocol. To offer mutual authentication between the server and client, they have used an asymmetric cryptosystem. This system is also resistant to malicious servers and fake terminals. The proposed protocol improves the security of user account information and personal privacy during the mobile-payment transaction process in comparison to existing approaches.

Distribution of Articles Based on the Classification of Cryptography Algorithms

This section focuses on modern encryption techniques such as ECC, RSA, and ASH256 asymmetric algorithms and the methods of their application and alignment with mobile payment channels.

Tafti et al. [17] aimed to enhance the security of the protocols used in the authentication process in mobile payments. The researchers proposed the GSM protocol to verify the authentication between the seller/store and the buyer/customer. The researchers used asymmetric encryption technology and session key transfer to provide authentication through mobile phone payment with NFC technology. The proposed protocol is composed of three different phases: "Authentication," "Authorization," and "Transaction." The researchers used two-way authentication to provide protection for both parties. The researchers also focused on reducing the exchanged messages between the two parties from five to four in order to provide synchronization in the resources of mobile phones. The researchers also focused on reducing key pairs. However, one of the problems that the researchers faced here was the increase in processing time in the authentication process between the two parties; this may elevate the time in the verification process.

Ma et al. [18] aimed to point out the use of payment technology via a two-dimensional QR code to facilitate mobile payments and to ensure the quality of information security in the exchange of authentication operations. The researchers used RSA encryption as a security solution to deal with various security problems due to the availability of this encryption in the length of the key between the two parties to document the payment process. The research lacks quality assurance of the security of the payment process via QR code and the improvement of mobile device payments.

Purnomo et al. [19] focused on providing the payment process using the QR code in order to preserve the users' information to provide the safety, integrity, and availability of data in the payment processes. The researchers aimed to provide security to the integrity of the data that was causing concern for users of electronic payment or payment by mobile phone. The researchers here refer to the implementation of the secure payment

process via QR code and the application of the asymmetric encryption algorithm using RSA to ensure the integrity of the data. This research invalidates the verification of bank accounts for the availability of the amount to be paid, and, as the researchers indicated, to the personal accounts they use to create this payment. This may cause a burden in the implementation of the payment due to adding money to this account or not guaranteeing the account used.

Ahmad et al. [20] here focused on payment via QR code by replacing the SHA256 cypher with an elliptical curve digital signature algorithm to ensure the integrity of the certificate for maintaining non-repudiation between the parties in the transmission process. The proposed system here has three levels: server verification, smart device, and barcode for the payment process. The steps that the payment process goes through here are simple and do not carry strong encryption to ensure the safety of payment between the buyer and the merchant. The payment process between the two parties passes through six stages, from creating the barcode process to completing the payment process. In notifying the merchant to complete the payment process via the server, the scheme used is a visual cryptography scheme (VCS) algorithm that is implemented between the customer and the seller (between two parties).

According to Zhou et al. [4], the static QR codes have various security problems and are simple to duplicate and alter. Even in a closed system, QR code payment still has security issues. In order to address the security issue with QR code payment, a dynamic QR code payment system that supports SM2, SM3, and SM4 cryptographic algorithms has been studied. This system can execute QR code scanning and scanned transactions, execute UnionPay cloud QuickPass transactions, and generate dynamic QR code information in real-time during the transaction process with one order and one code. The system makes use of SM3+SM2 signature computation and verification to make sure the firmware has not been tampered with and that its integrity and authenticity are guaranteed. To create data message digests, the SM3 algorithm, an upgraded version of SHA-256, is employed. The 512-bit message packet length and the 256-bit digest length are utilized with the Merkle-Damgard structure. The SM3 algorithm's construction is more complex even though its compression function is similar to that of SHA-256.

Lavanya et al. [5] stated that this approach has two stages of authentication: location authentication which preserves privacy, and device authentication. The privacy of the user is protected by encrypting the user's identity using physical layer encryption based on the user's location. For physical layer encryption, signatures such as channel condition information and carrier frequency offset are employed. The media access control (MAC) address is used for initial authentication in traditional procedures, and it is shared without encryption. To maintain privacy, the proposed technique encrypts MAC using a secret key generated from physical layer signatures using singular value decomposition (SVD). The secret key obtained using SVD is utilized for location authentication because it is location-specific and fluctuates depending on the location. Asymmetric key cryptography is used to perform user authentication, which is essential for mobile payment. For location authentication, physical layer signatures like Channel State Information (CSI) and Carrier Frequency Offset (CFO) are employed, while for device authentication, asymmetric key cryptography is utilized.

The SPPLAS algorithm, which is detailed in algorithms, is used to implement the PLS part of the suggested technique.

Yang et al. [21] referred to the offer of elliptic curve cryptography (ECC)-based efficient authenticated encryption technique. Because the suggested system does not require the creation of any digital signatures, computation costs can be significantly lowered. In addition, the researchers designed a secure electronic payment system using the suggested authenticated encryption approach. Confidentiality, authenticity, integrity, privacy protection, and double-spending prevention are all features of the proposed electronic payment system. The suggested authenticated encryption system can be simply deployed in mobile payment contexts, according to the findings of this research. It can also be used for an electronic auction, an online gathering, or electronic voting.

Ashrafi et al. [22] stated that the current rise in data-breaching events involving high-profile e-commerce organizations is concerning, as such risks to privacy can substantially impede electronic commerce's healthy expansion. The authors offer an e-payment technique that ensures authenticity while keeping the customer's sensitive information hidden from the parties participating in the online transaction. The suggested protocol allows consumers to anonymously purchase goods from an online merchant using a non-reusable password-based authentication mechanism, creating the optimal privacy environment in which to shop. The protocol is simple to implement in an e-commerce context and does not require significant changes to existing operations. The protocol also uses RSA algorithm to work.

The researchers' contributions also referred to the study and verification of anonymity during shopping, and they noted the verification of effective authentication of payment protocols and their advancement in authenticating credit cards in reducing detection or tampering with cards in the event of theft, and in enhancing

the use of a single session key to reduce fraud. In Figure 3 below, the research method and its workings are shown.

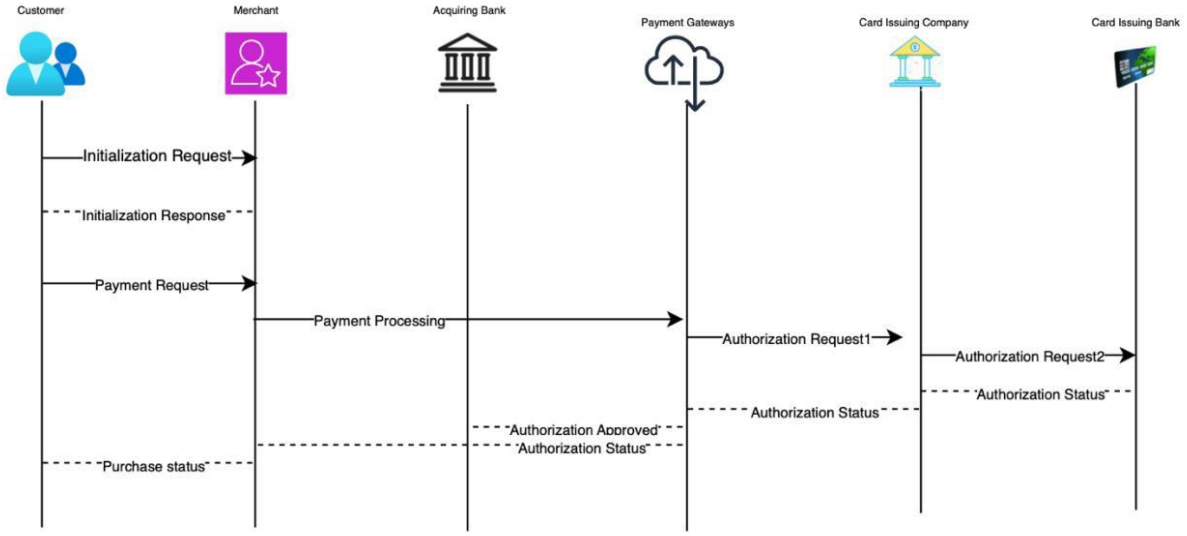

Figure 3. Message Exchange Proposed Method [21]

Prathama et al. [23] asserted that mobile payment systems are becoming more popular around the world, especially in Indonesia. However, the mobile payment system poses security vulnerabilities, including authentication, personal data, and the use of flawed cryptography. Chaudhry et al. [24]. claim to be able to circumvent these security problems using their elliptic curve cryptography system. This study implements the Chaudhry et al. [24] system and then compares it to the Indonesian mobile payment procedure. The results of the tests indicate that the implementation can provide privacy protection, authentication, access control, confidentiality, data integrity, non-repudiation, and double-spending prevention and that it is viable to execute in Indonesia. The researchers looked at banking information for beneficiaries in Indonesia.

Fun et al. [25] noted that the chance to make mobile devices a common payment mechanism for routine financial transactions is enormous given the current growth of wireless networks. Mobile payment is not yet widely accepted, unfortunately, due to issues including accountability features, privacy protection, and wireless network and mobile device restrictions. Furthermore, these protocols were developed to protect the vulnerable and user-risky traditional payment data flow. In this work, they provide a client-centric private mobile payment system that makes use of symmetric key operations. The results of this study can only be used as an initial comparison of privacy protection with other existing mobile payment protocols because privacy in electronic payment operations involves multiple parties, including the vendor, the buyer, and the bank for both sides in the payment process.

Secure Mobile Payment Scheme Based on Quick Response (QR) Code

This section focuses on the payment mechanism via the QR code and how it works with mobile payments. This section mentions many studies that have applied the study of payments via the QR code and their compatibility with the mobile phone.

Suryotrisongko et al. [26] looked at the use of payment technology using the quick response (QR) payment of the cooperative enterprise. The researchers studied the use of payment gateway (PG) by using the cryptographic hash function MD5 message-digest algorithm. After the forms are verified (valid password, etc.), PG will generate a 1024-bit RSA public-private key pair which is considered simpler than the quick response payment system and requires obtaining a certificate from the shopper and seller. This work pointed to the use of CBC ciphering mode with a Rijndael algorithm with a 128-bit block size. The user password acts as the Rijndael ciphering key.

The authors state that the system gives more convenience to the user as no internet or intranet connections are required and only a wireless intranet connection is needed for the shop to be able to communicate with the payment gateway (PG).

Ekundayo et al. [27] reviewed the use of the QR code in implementing the process of showing tourist information when scanning it to obtain information. Here, the researchers used the QR code in tourism in New Zealand to preserve archaeological tourist information and to facilitate its access to tourists without referring to

other parties or tour guides in this matter and to obtain more accurate and reliable information.

The researchers here used a technique in the implementation of this feature, which is the rapid response code and the technology of near-field communication. The researchers referred to the name of the system used in this process as QNBIS, as the proposed model was intended to preserve tourist information and access information faster and more accurately. However, this system is likely to face external intrusions when the information is stored in the databases which is to be obtained while scanning a QR code or NFC.

Kang et al. [28] focused on concealing the identity of the user to help reduce the publication of accusations or the imposition of illegal taxes on users through payments during public facilities and trains. This study proposes a privacy-preserving transit payment system based on traceable signatures, identity-based signatures, and anonymous signatures to protect passengers' privacy.

Focus of Mobile Payment Publications on Technological Factors and Hypothesis

Wireless and other associated technologies that are utilized to create and develop mobile payment services make up the technological environment. Some of these technologies, like transaction protocols and mobile network technology, advance gradually. Other technologies, like mobile handsets and their parts, have incredibly quick development cycles. Technology advancements provide more dependable, user-friendly, adaptable, and functionally-rich mobile payment services. As presented in this research, the most important encryption techniques that help in improving the quality of preserving the privacy of the mobile payment process were limited, and the studies that reasoned about the theories of forgetting the use of mobile payment operations were limited. As well, studies of the psychological and behavioral concerns of the individual were limited. The technical challenges were studied and counted in order to build the appropriate model for mobile payment operations.

DISCUSSION

This section will discuss collecting and analyzing previous studies on the adoption of mobile payment operations, which explain the most important factors affecting payment via mobile phones.

Recent Research and Performance of Mobile Payment Transactions

Mobile payment has become one of the most important means in the purchase process for several reasons, one of the most important of which is the speed of the process. There is no need to carry a credit card, coins, or paper money. One of the most important features needed for mobile payment is to hide the identity of the user while making payments without the need to know the other user's information. Other important potential concerns include the security and privacy of personal and important data in this type of account as well as the theft of smartphones in which this important data is stored.

In Figure 4, this review focuses on the aim of the research to study the extent to which the mechanism is applied and to identify modern security algorithms that help improve the quality of information preservation.

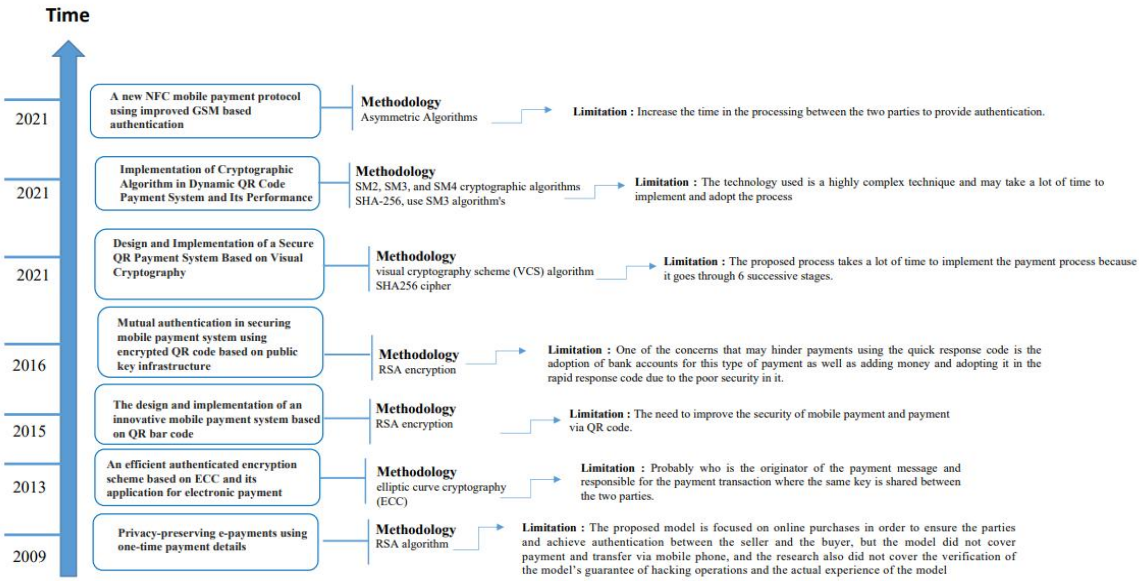

Figure 4. Privacy Preservation

In Table 1 and Figure 4, we refer to the framework of the problems related to the adoption of the user's intention to deal with payment by mobile phone and the problems related to payment by mobile phone.

We also look at the risks surrounding this aspect. Technology and security issues in mobile payments.

We have studied much previous literature and searched for the most important elements that affect mobile payments and the obstacles associated with them, especially after the increase in e-commerce. Table 1 presents an overview of the studies looking at the intention to pay via mobile phone and the security concerns that users face. The development of mobile devices, specifically, the development of mobile payment applications has not reached an advanced level. This may affect their primary goal of maintaining data privacy, specifically banking data. With such a large number of versions in the development of systems, there may be many gaps between the mobile phone system and the payment application system.

CONCLUSION

This paper described the factors affecting mobile payment adoption and privacy preservation. In the section adaptation of using a mobile payment system in the paper, we covered the aspects related to the first research question. The second research question was about the privacy technologies that are relied upon in payment via mobile phone, it was covered in the section privacy preservation in mobile payment.

There are several possible future research directions. First, researchers can gather more empirical data supported by guiding theories to form a better understanding of the underlying technology and enhance the quality and relevance of mobile payment research. We are not saying that conceptual papers are irrelevant or pointless. However, we think that further theory-based empirical research is required to improve our knowledge of the market for mobile payment services.

Second, practitioners steer technological advancement toward tighter collaboration with consumers and businesses. Third, our findings suggest that for mobile payment systems to flourish, their business models must change from being based on proprietary, constrained solutions to ones that are collaborative and standardized. Future research that maps mobile payment service attempts to the suggested framework and then provides a full review of each service would be beneficial for the practitioner community.

ACKNOWLEDGMENT

The authors gratefully acknowledge Qassim University, represented by the Deanship of "Scientific Research, on the financial support for this research under the number (COC-2022-1-2-J- 30624) during the academic year 1444 AH / 2022 AD".

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.

REFERENCES

[1] L. Y. Yan, G. W. H. Tan, X. M. Loh, J. J. Hew, and K. B. Ooi, "QR code and mobile payment: The disruptive forces in retail," *Journal of Retailing and Consumer Services*, vol. 58, p. 102300, 2021.

[2] P. De, K. Dey, V. Mankar, and S. Mukherjea, "An assessment of QR code as a user interface enabler for mobile payment apps on smartphones," in *Proceedings of the 7th Indian Conference on Human-Computer Interaction*, Dec. 2015, pp. 81-84.

[3] J. W. Lian and J. Li, "The dimensions of trust: An investigation of mobile payment services in Taiwan," *Technology in Society*, vol. 67, p. 101753, 2021.

[4] Y. Zhou, B. Hu, Y. Zhang, and W. Cai, "Implementation of cryptographic algorithm in dynamic QR code payment system and its performance," *IEEE Access*, vol. 9, pp. 122362-122372, 2021.

[5] D. L. Lavanya, R. Ramaprabha, B. Thangapandian, and K. Gunaseelan, "Novel privacy preserving authentication scheme based on physical layer signatures for mobile payments," *SN Computer Science*, vol. 2, no. 2, p. 119, 2021.

[6] S. Bojjagani, V. N. Sastry, C. M. Chen, S. Kumari, and M. K. Khan, "Systematic survey of mobile payments, protocols, and security infrastructure," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 1, pp. 609-654, 2023.

[7] Juniper Research. "Mobile Contactless Payment Transaction Volumes to Grow by 92% Globally by 2023." Juniperresearch.com. https://www.juniperresearch.com/press/mobile-contactless-payment-transaction-volumes (accessed Apr. 8, 2024).

[8] 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," *Technological Forecasting and Social Change*, vol. 146, pp. 931-944, 2019.

[9] T. Ganesan, T. S. Ong, W. P. Cheah, and T. Connie, "Assessment of security risk impact on mobile payment services," in *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, Sep. 2020, pp. 1-6.

[10] A. Pešterac and N. Tomić, "Loss of privacy in electronic payment systems," *Anali Ekonomskog fakulteta u Subotici*, no. 43, pp. 135-149, 2020.

[11] N. El Madhoun and G. Pujolle, "Security enhancements in EMV protocol for NFC mobile payment," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 1889-1895.

[12] S. Sung, "A new key protocol design for cryptocurrency wallet," *ICT Express*, vol. 7, no. 3, pp. 316-321, 2021.

[13] W. Yang, J. Li, Y. Zhang, and D. Gu, "Security analysis of third-party in-app payment in mobile applications," *Journal of Information Security and Applications*, vol. 48, p. 102358, 2019.

[14] F. Zamanian and H. Mala, "A secure and efficient mobile payment protocol with fair-exchange feature," in *2020 25th International Computer Conference, Computer Society of Iran (CSICC)*, Jan. 2020, pp. 1-8.

[15] S. S. Ahamad and A. S. K. Pathan, "Trusted service manager (TSM) based privacy preserving and secure mobile commerce framework with formal verification," *Complex Adaptive Systems Modeling*, vol. 7, pp. 1-18, 2019.

[16] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, "Secure authentication protocol for mobile payment," *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 610-620, 2018.

[17] F. S. M. Tafti, S. Mohammadi, and M. Babagoli, "A new NFC mobile payment protocol using improved GSM based authentication," *Journal of Information Security and Applications*, vol. 62, p. 102997, 2021.

[18] 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 *2015 International Conference on Network and Information Systems for Computers*, Jan. 2015, pp. 435-440.

[19] 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 *2016 6th International Conference on System Engineering and Technology (ICSET)*, Oct. 2016, pp. 194-198.

[20] L. Ahmad, R. Al-Sabha, and A. Al-Haj, "Design and implementation of a secure QR payment system based on visual cryptography," in *2021 7th International Conference on Information Management (ICIM)*, Mar. 2021, pp. 40-44.

[21] J. H. Yang, Y. F. Chang, and Y. H. Chen, "An efficient authenticated encryption scheme based on ECC and its application for electronic payment," *Information Technology and Control*, vol. 42, no. 4, pp. 315-324, 2013.

[22] M. Z. Ashrafi and S. K. Ng, "Privacy-preserving e-payments using one-time payment details," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 321-328, 2009.

[23] D. R. Prathama, P. A. W. Putro, and D. I. Naviangga, "Secure mobile payment based on elliptic curve cryptography," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Nov. 2018, pp. 140-145.

[24] S. A. Chaudhry, H. Naqvi, M. S. Farash, T. Shon, and M. Sher, "An improved and robust biometrics-based

three factor authentication scheme for multiserver environments," *The Journal of Supercomputing*, vol. 74, no. 8, pp. 3504-3520, 2018.

[25] T. S. Fun, L. Y. Beng, J. Likoh, and R. Roslan, "A lightweight and private mobile payment protocol by using mobile network operator," in *2008 International Conference on Computer and Communication Engineering*, May 2008, pp. 162-166.

[26] H. Suryotrisongko and B. Setiawan, "A novel mobile payment scheme based on secure quick response payment with minimal infrastructure for cooperative enterprise in developing countries," *Procedia-Social and Behavioral Sciences*, vol. 65, pp. 906-912, 2012.

[27] S. Ekundayo, O. Baker, and J. Zhou, "QR code and NFC-based information system for Southland tourism industry-New Zealand," in *2020 IEEE 10th International Conference on System Engineering and Technology (ICSET)*, Nov. 2020, pp. 161-166.

[28] J. Kang and D. Nyang, "A privacy-preserving mobile payment system for mass transit," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 8, pp. 2192-2205, 2017.