Journal of Electronics and Informatics (ISSN: 2582-3825)
www.irojournals.com/iroei/

Analysis of Hybrid Securing Digital Payment System through Risk Perception

C. Vijesh Joe

Assistant Professor (SG-1), SCOPE-Analytics, VIT Vellore Campus, India

E-mail: vijesh.joe@gmail.com

Abstract

This study article discusses a novel method of electronic payment wherein a retailer is made incapable of obtaining a customer's payment details which therefore accomplishes a secure transaction. Customers' payment information, often a credit or debit card detail, faces a number of security issues when transmitted to a retailer via the Internet. Credit card data theft, credit card fraud, and data manipulation are all potential threats. A company has the option of either using or storing client information. If a retailer does not take enough precautions to protect its server or system against data thieves, spammers, spyware, malware, and hackers, then their customers' information might be stolen and exploited. The main parts included in this research work are transaction through token issuance and Pedersen commitment approach to provide better efficacy of successfully securing digital payment system. The usual data security requirements are followed by payment gateways, and the most secure techniques and technologies are used when communicating with banks and credit card firms.

Keywords: Mobile payment service, online payment, electronic payment, digital payment security

1. Introduction

In 1990 [1], e-commerce was offered as a novel method to the consumer and corporate communities. The growth and refinement of e-commerce have brought significant advantages to consumers and businesses throughout the globe. The evolution of the Internet parallels the development of electronic commerce. Online purchasing was made feasible with the public launch of the Internet in 1991 [1,2]. This includes buying and selling products and services as well as sharing data and information. Customers may use their cellphones as a form of payment while purchasing online thanks to mobile payment systems [4,5]. An

DOI: https://doi.org/10.36548/jei.2022.4.001
Received: 11.09.2022, received in revised form: 07.10.2022, accepted: 22.10.2022, published: 01.11.2022

essential e-commerce add-on, "portable business" [6] allows consumers to engage in online commercial transactions utilising portable wireless handheld devices like tablets, smartphones, and laptops. Since clients can buy from the comfort of their own homes, at reduced rates, and with the convenience of having their purchases delivered directly to their doorsteps, e-commerce is gaining in popularity.

E-meteoric commerce's rise to prominence is largely due to the convenience and accessibility of doing business online. It facilitates the instantaneous transfer of capital between companies and the global marketplace [7]. Because of the global reach of the Internet, many people are eager to launch their own business websites. Customers are drawn to internet retailers because they provide a convenient alternative to physically visiting stores, something many of them would rather not do. It consists of making and receiving financial transactions using wireless connections [8-10]. Figure 1 shows various parameters of securing digital payment system.

Figure 1. Securing digital payment system [28]

Information technology is employed in e-commerce as a result of the rapid development of computer networks and the Internet. A wide variety of e-commerce solutions may be accessed online. Thus, a method of making electronic payments is essential for online trade. Consequently, the acceptance of electronic payments is a major challenge for the future of e-commerce [11].

Recently, the rise of online banking and retail has contributed to the expansion of electronic payment systems. Online payment systems and other transaction processing gadgets are expanding as a result of global technology development. A payment gateway is a

company that facilitates financial transactions between consumers, businesses, and financial institutions over the Internet. It aids in keeping a purchase and the shopper's financial details safe throughout the transaction. In order to protect sensitive data during transmission between a customer and the transaction processor, a payment gateway employs encryption. Several methods are suggested to assist in making the connection between the client and the online payment or merchant gateway safe. Online shoppers in particular, need to know that their sensitive information, such as credit card numbers, is safe from prying eyes. As a result, a safe connection is required for making purchases online. The most common forms of online fraud are phishing and identity theft [12,13].

2. Literature Survey

2.1 Next-Generation Payment Instruments

In the grand scheme of economic and technical developments, mobile payment is a newcomer. Due of the increasing number of people who use smartphones, financial service companies now have a chance to gain efficiency and market share. Users of financial services now have easier access to such services. Despite the obvious merits of this innovative financial product, it has not been adopted at the rate that was expected. Only 8% of people in the world actually use their mobile phones, although 96% of people in the world have a mobile phone subscription [13]. It can be shown that only a small fraction of the world's registered mobile phone users actually makes use of mobile payment services. However, this work demonstrates that there are fresh openings for expanding and promoting these payment methods.

Electronic payment systems have mostly supplanted cash transactions in recent years. From both a technological and user acceptability perspective, digital payments have been the subject of much study. Researchers are interested in a wide range of topics related to mobile services, including user satisfaction, network operators, consumer acceptance, consumer continued use behaviour, and stakeholders' expectations [14]. Based on the data, it seems that research on digital payment systems has grown in both scope and frequency of publication during the previous two decades. Even though there are many studies on the subject of digital payment variations, investigations on the factors that influence digital prices have shown contradictory results. More in-depth research on the usage of these tools is necessary, as is the ongoing tracking of how different financial solutions influence consumers' outlooks and routines. This makes it crucial to reflect on prior knowledge.

There is a dearth of scholarly investigations into how people feel about the security of digital transactions, despite the many studies on the topic. Numerous research topics have already been examined in the field of digital pricing, as evidenced by a survey of the existing literature on the topic. As such, the study served as a survey of the relevant literature, fostering growth in the subject and pointing the way toward new avenues of inquiry. This is an excellent synopsis of the studies done in this field. The paper also addressed the implications for service providers and regulators of the digital payment industry of the directions the future research should take [15].

Furthermore, Kartika et al. [16] claimed that bolstering the security and privacy of data during cashless financial transactions is crucial to promote these services in smart cities. Customers are finding it harder to exercise their rights in e-commerce, as noted by Yang et al. [17], owing to legislative gaps in data protection. Customers' concerns about their personal information being misused and their ability to make secure financial transactions are amplified by the lack of clarity in regulations around mobile payment systems. Trust, perceived risk, and their impact on consumer happiness continue to be issues in e-commerce, even as the technology improves, as El Haddad et al. [18] point out.

2.2 Summary of the Problem Statement

To this day, one of the most common ways for customers' personal information to be stolen from the e-commerce system is via the transmission of their payment details to a merchant's payment gateway, despite the existence of security measures. A merchant may still keep the encrypted payment details of his customers and decode them at a later time. In the event of a chargeback or dispute, the existing payment systems enable the retailer to collect the customer's payment details in order to assert the legitimacy of the transaction. A merchant may verify the legitimacy of a transaction using other means than a customer's payment details. A transaction's legitimacy may be established with the use of other purchase-related data.

3. Hybrid Securing Digital Payment System

3.1 Proposed Approach

The current number of users is adequate, and mobile payment options will only make it grow. However, the network infrastructure, which is crucial to the success of such solutions, will eventually feel the strain of this expansion. As a result, how the development

of next-generation networks may affect mobile payment options is investigated in this work. There may be fewer mobile payment alternatives and methods to alleviate difficulties by enhancing the network, if more about the present obstacles is studied [19 -21].

3.2 Breakdown of How a Payment System Works

The current payment mechanism typically consists of the following steps:

- A buyer goes to a store's online storefront and browses the merchandise before deciding which ones to purchase. Those things are now in his virtual shopping basket.
- b) At checkout, a consumer provides his financial details in order to complete the purchase. Customers' debit and credit card details are examples of payment information.
- c) The buyer's financial data is sent by the seller to a payment gateway for verification and authorization.
- d) The customer's payment information is verified by the gateway, and if everything is seemly, the transaction is approved. The message containing the payment capture token indicates that the charge has been approved by the merchant.
- e) The retailer ships the goods to the buyer and submits a payment request via the gateway. To request payment for a transaction, a retailer will typically transmit the relevant payment capture data over the payment gateway.
- f) The merchant's payment capture details are verified by the payment gateway. When everything is seemly, the gateway transfers the funds to the retailer.

3.3 Risk perception

Out of the reviewed articles, this is the shortest one that expands upon the understanding of potential threats to confidentiality and privacy. Trust in a digital payment app's developer comes mostly from the user's perception of the developer's commitment to the user's privacy and security. Identity theft and information exploitation are just two of the many threats that consumers face while shopping online. Examples include companies using customers' personal information for marketing purposes without their knowledge or consent. This makes sense considering that a person's unique and valuable identity in the digital world is built on a foundation of both financial and personally identifiable information. Popular beliefs about safety are recorded in the literature [22 - 25].

3.4 Security and Privacy

Several empirical investigations have taken a customer-centric approach to the topic of security and privacy, finding that concerns about these two factors have a substantial (direct or indirect) bearing on people's propensity to use and promote digital technology. Previous research has shown that even in an uncertain and even dangerous online setting, trust can flourish and is vital. Trust between a trustor (a customer) and a trustee (a seller) is a powerful motivator in retail settings because it increases repurchase intent and decreases perceived risk. Users are more likely to provide non-sensitive information like preferences than sensitive information like account or credit card data. Another factor in whether or not a customer would make a financial or personal information transfer online is the level of confidence they have in the online service provider [26].

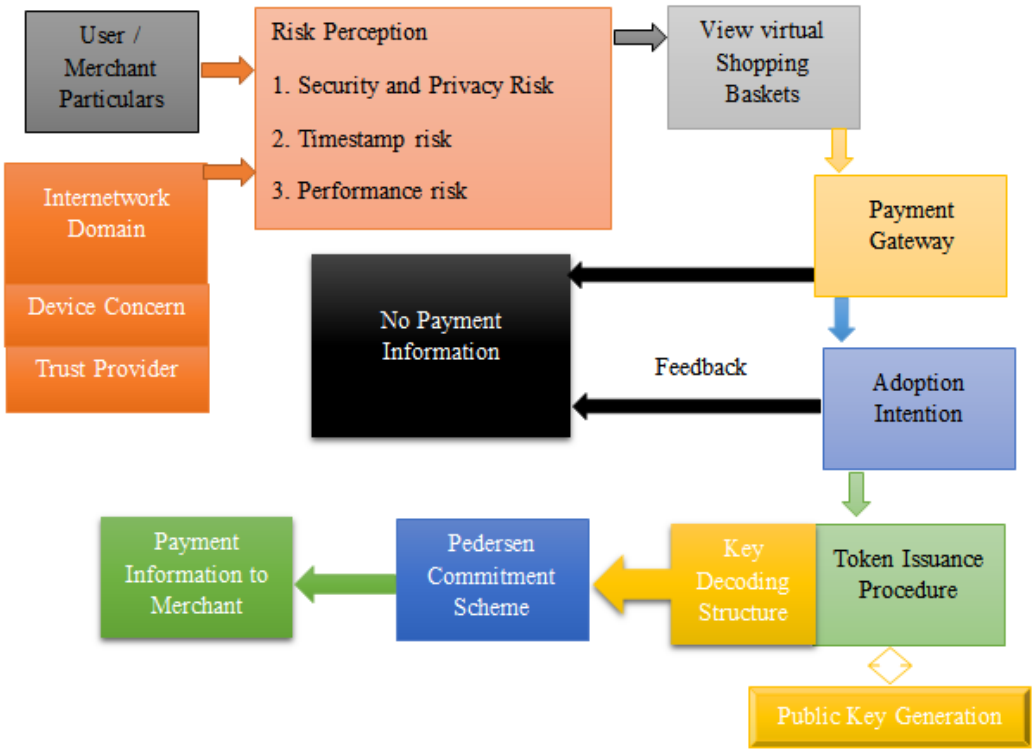

Figure 1. Proposed design framework

3.5 Payment Information Concealed from the Store

Merchants keep certain client data and transaction details after a consumer pays via a payment gateway, such as the customer's name and address. Some payment data, such as card type or issuer, last four digits, or encrypted credit or debit card details, may be stored by businesses under the present payment system setup. This is done so that businesses have concrete evidence of a transaction's legitimacy in the event of a chargeback [27]. However,

several difficulties arise when clients provide payment information to a payment gateway rather than the merchant.

- The merchant must be recognised and verified as legitimate by the payment gateway.
- The legitimacy of a transaction should be verified by a payment gateway before funds are released to the retailer.
- It is the responsibility of the payment gateway to ensure that funds are sent to the correct merchant; also, it is the merchant's responsibility to collect customer purchase details and evidence in the event of a chargeback or dispute.

3.6 Pedersen Commitment Scheme

By leveraging the unsolvability of the discrete logarithm problem, the Pedersen Commitment scheme provides an unconditionally concealed and computationally binding commitment method. It's a subset of cryptographic commitment that lets you pledge to anything without broadcasting your secret and without giving up your right to expose it later. Because of this characteristic of a Pedersen promise, this proposed payment system is safe from attackers who steal money from legitimate businesses while pretending to process legitimate transactions. In addition, it aids in resolving the most pressing design challenge of providing a means for retailers to monitor and verify the veracity of transactions in the event of chargebacks and other challenges.

3.7 Transaction Token Issuance

An identity provider may offer a transaction token to a business owner to use in a particular transaction. When a vendor sends a message asking for a token to use in a transaction, this object is generated in response. Therefore, when an IP gets a message requesting a transaction token, it decrypts the message using its private key to reveal the encrypted identity property and the merchant ID. The identity provider verifies the merchant's registration and retrieves the merchant's public key using the provided ID. A public key is used to decode the identification attribute for the IP [28].

4. Comparative Observations

4.1 Robustness and Efficiency

In light of the rapid evolution taking place in the realm of electronic payments, it is essential to evolve and adapt. Time-to-market robustness is critical for gauging a system's

performance in competitive conditions. All electronic payment systems' security features should undergo rigorous testing overseen by the threat monitoring function to guarantee their reliability and efficacy. The banking industry around the globe has mushroomed in response to the proliferation of new methods of making and receiving monetary transactions. Online banking has been used by financial institutions as a means of increasing efficiency and productivity and, by extension, lowering costs [22]. One of the benefits of the electronic payment system is its efficiency [9]. Electronic payment is growing in popularity among major merchants because it increases customer happiness by making the purchasing process more secure, more convenient, and more exciting for the consumer. E-wallets are becoming more popular among customers because of the convenience they bring to everyday transactions [23]. Reducing transaction costs and facilitating trade on commodities and services with considerably lower values may significantly increase efficiency. The data given into the system must be verified for accuracy, is the recommendation that might improve the efficiency of online payment: The highest robustness has been proved with the hybrid proposed framework, which is shown in table 1.

Table 1. Proposed Hybrid model for Online and Offline mode

Model Design	**Transaction (banking Mode)**		**Attack Type**	**Transaction Gateway**	**Robustness**
	Online	**Offline**			
Traditional Artificial Learning Method	Available	Not Available	Fake UPI link OTP fraud Malware	Electronic Payment	Medium
Pedersen commitment + Token Issuance Scheme	Available	Available	Fake UPI link OTP fraud Malware	Digital Electronic Payment	Strong

4.2 Important Factors

There are many unexplored aspects that affect how people see danger. For example, a company's standing in the market may be an important indicator of whether or not a customer will trust its digital payment services, and banks, and other financial institutions may want to encourage customers to feel safe making online purchases by encouraging them to adopt payment methods that adhere to government regulations and international standards such as

overall efficiency and accuracy through risk perception. While most research has concentrated on the retail sector, concerns and risks vary widely across other sectors. This is a must-study area for the foreseeable future. The above said important factors are measured with the individual scheme as shown in the following table 2.

Table 2. Obtained Results for Risk perception

Model Design	Transaction (banking Mode)		Overall Efficiency	Accuracy	Risk Perception
	Online	Offline			
Pedersen Commitment	Available	Available	High	Medium	Yes
Token Issuance Scheme	Available	Available	High	High	Not Considered

4.3 Payment Information to Merchants

Because of these risks, it's clear that when businesses submit customers' financial details to payment gateways, that data travels across even more networks, increasing its vulnerability to breaches and assaults. As a result, a new strategy is devised to protect payment systems in which clients submit their financial data directly to gateways. In this method, the seller is compensated for his wares without ever seeing the buyer's credit card details, not even in hashed or encrypted form.

5. Discussion

Mobile payment systems arose swiftly for the same reason as the proliferation of other technologies used to facilitate everyday life throughout the globe. There is no longer a need to spend a day at the bank to do which can be done in a few clicks with the help of the smartphone and the associated payment infrastructure. While this convenience is welcome, it has also brought with it a number of risks, the most serious of which being the possibility of criminals compromising the payment system in order to steal money. Cryptocurrency exchanges built on blockchain technology, once thought to be the safest form of digital payment, have recently fallen victim to hacking, signalling that, cybercriminals are becoming better at finding security flaws. Affluent research might be done in the future into this new arena where good and bad people battle over how to make mobile payment systems safer and more secure against new threats.

There's always room for development and progress in every area. The plan's main goal is to learn why people use (or don't use) a particular technology-enabled service, based on their own preferences. Designing services that are economically sustainable and beneficial to customers and other ecosystem participants is of paramount importance. Mobile phone use is widespread, and most people always have one within reach. The majority of business, commerce, and communication now takes place on mobile devices. As a result, a plethora of companies now provide solutions tailored specifically to mobile devices. Mobile phone payment options exist, but they have higher security requirements than most others.

6. Conclusion

The vast majority of modern-day payment systems are account-based payment systems that prioritise security, privacy, secrecy, and authentication. This article has covered a variety of payment methods, including their applications, enabling technologies, and security measures. In addition, it has provided a summary of Mobile Payment System (MPS) and its many parts. Finally, a comprehensive overview of the MPS's origin, evolution, and current state of implementation is provided. This study recommends further research into the following areas based on its examination of the connection between technological progress and MPS security performance, by identifying and understanding the rate of technological change in MPS environments and developing a dynamic strategy concerning platform design for an overall MPS security improvement and creating a continuous monitoring process for advanced knowledge of payment scheme markets. This research gives theoretical insights on the roles of the platform and technology in ensuring the safety of MPS users, which is helpful in understanding how this recent shift in user perception of security impacts the MPS user experience as a whole. Ideas for how MPS service providers should shape their offerings in response to consumers' subjective and objective perceptions of the MPS security landscape are also presented.

References

[1] Lee, W.H.; Miou, C.S.; Kuan, Y.F.; Hsieh, T.L.; Chou, C.M. A peer-to-peer transaction authentication platform for mobile commerce with semi-offline architecture. Electron. Commer. Res. 2018, 18, 413–431.

[2] Yang, W.; Li, J.; Zhang, Y.; Gu, D. Security analysis of third-party in-app payment in mobile applications. J. Inf. Secur. Appl. 2019, 48, 102358.

[3] AL-Khaleefa, A.S.; Ahmad, M.R.; Isa, A.A.M.; Esa, M.R.M.; Aljeroudi, Y.; Jubair, M.A.; Malik, R.F. Knowledge Preserving OSELM Model for Wi-Fi-Based Indoor Localization. Sensors 2019, 19, 2397.

[4] Wang, J.; He, Q.; Han, Q. Research on Internet Payment Security Based on the Strong Authentication of the Timeliness and Multi-factors. In Proceedings of the 2016 7th International Conference on Education, Management, Computer and Medicine (EMCM 2016), Shenyang, China, 29–31 December 2016; pp. 19–23, 59.

[5] Okpara, O.S.; Bekaroo, G. Cam-Wallet: Fingerprint-based authentication in M-wallets using embedded cameras. IEEE Int. Conf. Environ. Electr. Eng. 2017.

[6] Gode, P.; Nakhate, S.T.; Mane, S.S. Authentication for Mobile Banking by using Android based Smart Phones. Imp. J. Interdiscip. Res. 2017, 3, 1314–1318.

[7] Khachane, D.; Sant, Y.; Sachan, Y.; Ghodeswar, A. Enhancing Security of Internet Banking Using Biometrics. J. Comput. Eng. 2018, 20, 22–25.

[8] Elliot, M.; Talent, K. A robust and scalable four factor authentication architecture to enhance security for mobile online transaction. Int. J. Sci. Technol. Res. 2018, 7, 139–143.

[9] Alibabaee, A.; Broumandnia, A. Biometric Authentication of Fingerprint for Banking Users, Using Stream Cipher Algorithm. J. Adv. Comput. Res. 2018, 9, 1–17.

[10] Khatib, S.F.A.; Abdullah, D.F.; Hendrawaty, E.; Elamer, A.A. A bibliometric analysis of cash holdings literature: Current status, development, and agenda for future research. Manag. Rev. Q. 2021, 1–38.

[11] Hazaea, S.A.; Zhu, J.; Al-Matari, E.M.; Senan, N.A.M.; Khatib, S.F.A.; Ullah, S. Mapping of internal audit research in China: A systematic literature review and future research agenda. Cogent Bus. Manag. 2021, 8, 1938351.

[12] Zamil, I.A.; Ramakrishnan, S.; Jamal, N.M.; Hatif, M.A.; Khatib, S.F.A. Drivers of corporate voluntary disclosure: A systematic review. J. Financ. Report. Account. 2021, ahead of print.

[13] Hazaea, S.A.; Zhu, J.; Khatib, S.F.A.; Bazhair, A.H.; Elamer, A.A. Sustainability assurance practices: A systematic review and future research agenda. Environ. Sci. Pollut. Res. 2022, 29, 4843–4864.

[14] Block, J.H.; Fisch, C. Eight tips and questions for your bibliographic study in business and management research. Manag. Rev. Q. 2020, 70, 307–312.

[15] Khatib, S.F.A.; Abdullah, D.F.; Elamer, A.A.; Abueid, R. Nudging toward diversity in the boardroom: A systematic literature review of board diversity of fifinancial institutions. Bus. Strateg. Environ. 2021, 30, 985–1002.

[16] Kartika, H.; Fatimah, Y.A.; Supangkat, S.H. Secure Cashless Payment Governance in Indonesia: A Systematic Literature Review. In Proceedings of the 2018 International Conference on ICT for Smart Society (ICISS), Semarang, Indonesia, 10–11 October 2018; pp. 1–4.

[17] Yang, Y.; Liu, Y.; Li, H.; Yu, B. Understanding perceived risks in mobile payment acceptance. Ind. Manag. Data Syst. 2015, 115, 253–269.

[18] El Haddad, G.; Aimeur, E.; Hage, H. Understanding Trust, Privacy and Financial Fears in Online Payment. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 28–36.

[19] G. Ali, M. Ally Dida, A. Elikana Sam, Two-factor authentication scheme for mobile money: A review of threat models and countermeasures, Future Internet 12 (10) (2020) 160.

[20] D. Kunda, M. Chishimba, A survey of android mobile phone authentication schemes, Mobile Networks and Applications (2018) 1–9.

[21] F. S. G. Talom, R. K. Tengeh, et al., The impact of mobile money on the financial performance of the smes in douala, cameroon, Sustainability 12 (1) (2019) 1–1.

[22] Talwar, S.; Dhir, A.; Khalil, A.; Mohan, G.; Islam, A.K.M.N. Point of adoption and beyond. Initial trust and mobile-payment continuation intention. J. Retail. Consum. Serv. 2020, 55, 102086, doi:10.1016/j.jretconser.2020.102086.

[23] Dehghanpouri, H.; Soltani, Z.; Rostamzadeh, R. The impact of trust, privacy and quality of service on the success of E-CRM: The mediating role of customer satisfaction. J. Bus. Ind. Mark. 2020, 11, 1831–1847, doi:10.1108/JBIM-07-2019-0325.

[24] Fan, X.; Zhao, W.; Zhang, T.; Yan, E. Mobile payment, third-party payment platform entry and information sharing in supply chains. Ann. Oper. Res. 2020, doi:10.1007/s10479-020-03749-8.

[25] Park, S.; Kim, Y.; Chang, H. An empirical study on security expert ecosystem in the future IoT service environment. Comput. Electr. Eng. 2016, 52, 199–207, doi:10.1016/j.compeleceng.2016.04.001.

[26] Ahn, K.; Cho, J.-S. Major concerns of FinTech (Financial Technology) services in the Korean market. J. Bus. Retail. Manag. Res. 2019, 14, 123–133, doi:10.24052/jbrmr/v14is01/art-11.

[27] Singh, N.; Sinha, N. How perceived trust mediates merchant's intention to use a mobile wallet technology. J. Retail. Consum. Serv. 2020, 52, 101894, doi:10.1016/j.jretconser.2019.101894.

[28] Dijesh, P.; Babu, S.S.; Vijayalakshmi, Y. Enhancement of e-commerce security through asymmetric key algorithm. Comput. Commun. 2020, 153, 125–134.

[29] Website: https://renierbotha.com/2019/01/05/cyber-security-101-for-business-owners/

Author's biography

C. Vijesh Joe is presently working as Data Scientist at WoTo Technologies in Chennai. His major area of research includes cloud computing, speech processing, wireless networks security, data science analytics, and computer graphics in multimedia.