ISSN 2089-8673 (Print) | ISSN 2548-4265 (Online)
Volume 13, Issue 2, July 2024

ELECTRONIC PAYMENT THREATS AND SECURITY: A SYSTEMATIC LITERATURE REVIEW

Amelia Citra Dewi[1], Erik Iman Heri Ujianto[2], Rianto Rianto[3]

[1,2,3] Master of Information Technology, Universitas Teknologi Yogyakarta, Indonesia

email: ameliacitradewi@gmail.com[1], erik.iman@uty.ac.id[2], rianto@staff.uty.ac.id[3]

Abstract

In the emerging field of electronic payment systems, security challenges have become a major concern. This research addresses a comprehensive understanding of mitigation strategies for these threats. Through systematic literature analysis, we investigated the security vulnerabilities in electronic payment processes and discovered the latest blockchain technology as a strengthened security framework. Our findings reveal that while encryption and authentication provide the foundation of security, the integration of blockchain technology offers an unprecedented level of transaction integrity and transparency. This research not only highlights the urgent need for electronic payment security measures but also highlights the potential of blockchain and machine learning as transformative solutions. The implications of our research indicate an important shift in payment systems towards more secure and resilient electronic systems, paving the way for future research to explore the integration of cutting-edge technologies in combating ever-evolving cyber threats by leveraging blockchain technology, quantum computing and machine learning.

Keywords : electronic payment, e-payment, literature, mobile payment, m-payment, review
X`

Received: 20-03-2024 | **Revised:** 24-05-2024 | **Accepted:** 03-06-2024
DOI: https://doi.org/10.23887/janapati.v13i2.76635

INTRODUCTION

Electronic transactions in Indonesia for 2013-2022 experienced a significant increase of 13,900%. In 2022, electronic transactions will increase to 407.5 trillion rupiah from 2.9 trillion rupiah in 2013. This is influenced by the initiation of the national non-cash movement (*Gerakan Nasional Non Tunai* / GNNT) issued by the central bank in 2014 [1].

To this day, almost all transactions in the trade sector that were previously carried out conventionally using cash have been replaced by electronic payments. In Indonesia, e-wallet such as Gopay, OVO, and Dana are also growing for non-commercial purposes, such as paying school fees, electricity, health, and so on [1]. Electronic payments first appeared as a third-party payment system that bridged buyers and sellers in electronic commerce [2]. In practice, the development of internet infrastructure is crucial to the electronic payment process [3]. In the digital transformation era, seamless electronic payments can minimize the time and effort required for users to make transactions.

Many types of devices can be used for electronic payments, such as smartphones, smartwatches, etc. In general, electronic payments are defined as transactions carried out using electronic devices, starting from initiating transactions to authorizing and completing financial transactions. Although electronic payments offer convenience and efficiency, implementing this payment system can also negatively impact user security and privacy. Personal information or data contained in electronic payments and recorded user transaction habits are vulnerable to cybercrime and can be misused [4].

From 2017 to 2022, Indonesia recorded 486.000 reports of criminal acts related to violations of information and electronic transactions. Among them, 405.000 cases were online transaction fraud, followed by 19.000 cases of fictitious online investment fraud, and 12.000 cases of fraud in electronic buying or selling transactions [5]. The main threats in electronic payments are the leakage of personal data and illegal access to users' financial accounts [6].

Electronic payment systems not only play a role in completing transactions, but also have important factors for maintaining security, including protecting sensitive user information, preventing fraud, and ensuring that transactions are carried out with high integrity. In real conditions, electronic payments must include several principles to ensure cyber security, such as: Authentication, Integrity, Availability, Confidentiality, and Accountability. These fundamentals can also add up, depending on the type of attack or cybersecurity that occurs [3]. Therefore, security in electronic payments are crucial for continuously evolving and withstanding new threats.

Several studies have discussed security aspects in electronic payments, such as data encryption techniques [7], authentication protocol [4], and anti-fraud detection methods [3]. Solutions related to this security aspect have also been proposed, including the development of encryption algorithms [8], authentication protocols with biometrics [4], and the development of machine learning to detect fraud [9]. It is necessary to synthesize the findings of several of these studies to give a more thorough grasp of the threats, solutions, and development of electronic payment security systems. However, there are still gaps that need to be closed, especially in integrating new technologies such as blockchain and machine learning to secure electronic payments. Apart from that, it has not been explicitly defined in previous research regarding the definition and what things are considered a security breach in electronic payment security. There was also a notable gap where studies were conducted based on the conditions in the researcher's country. There were limitations in systematic research that gathered electronic payment studies from other countries. Parmar and Machhar study a literature review on adopting e-payment systems in India, analyzing various electronic databases up to April 2022. In the Indian context, the adoption of e-payment systems has increased following the COVID-19 pandemic, driven by an increase in online activity and the number of Internet users. Despite concerns about security risks, increasing technological awareness among Indian society has encouraged accepting e-payment systems. This study concludes that trust factor plays a crucial role in the adoption of e-payment systems and emphasizes the need for additional research using qualitative data to comprehend the variables affecting e-payment system adoption in India [10]. Susanto *et al.* examine the surge in digital payment usage across Asia. This surge is attributed to the widespread availability of internet services and the increased functionality of gadgets, leading to the growth of various digital payment methods such as mobile payments, internet banking, QR Codes, and electronic payments. The research analyzes 597 articles on digital, electronic, and mobile payments and finds significant factors influencing digital payment adoption, including trust, perceived risk, satisfaction, and security. The study notes that the impact of these factors can vary based on the digital payment products, user demographics, and research methodologies employed [11]. Although both studies contribute to their domains, there still needs to be more integrated research on electronic payments on a global scale.

Encompassing a global perspective, this systematic literature review includes studies from other countries with well-established electronic payment systems. This approach broadens the scope of analysis and provides insights into best practices and common challenges encountered by electronic payment systems worldwide. By combining experiences from different countries, it becomes possible to assess the applicability and potential adoption of adequate security measures within the electronic payment landscape. This research aims to comprehensively analyze the advantages and limitations of different electronic payment systems while analyzing major security threats and highlighting the essential security properties their systems should comply with. Consequently, the literature review aims to draw on global opportunities for further enhancement in electronic payment security in the future.

METHOD

In this research, the literature review process was conducted using the Kitchenham method to identify studies related to electronic payment security. By employing this guideline, the systematic literature review is divided into 3 stages: planning, conducting, and reporting, with several steps described in Figure 1 [12].

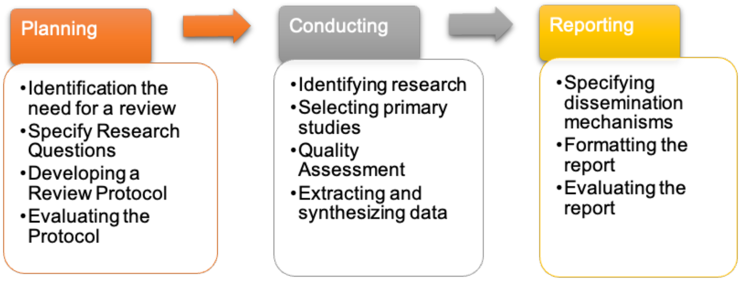
Planning
•Identification the need for a review
•Specify Research Questions
•Developing a Review Protocol
•Evaluating the Protocol
Conducting
•Identifying research
•Selecting primary studies
•Quality Assessment
•Extracting and synthesizing data
Reporting
•Specifying dissemination mechanisms
•Formatting the report
•Evaluating the report

Figure 1. Systematic Literature Review stages by Kitchenham and Charters

In the first stage, the research questions should be formulated based on the chosen research topic. In this study which focuses on electronic payment security, the research questions aim to understand electronic payments and their associated security threats, as well as potential mitigation measures, to lay a new foundation for developing safer electronic payment systems in the future. There are three research questions (RQ) that will be discussed as follows:

1. RQ 1: “What are the identified threats ans security breaches in the research articles that can occur in the electronic payment process?”
2. RQ 2: “What security methods are suggested to minimize the potential threats or enhance electronic payment security?”

After identifying the research questions, the process continues by developing the review protocol. The literature search was conducted in November 2023 using the Publish or Perish software, with Google Scholar selected as the database. It was decided that the research paper would only utilize literature published within the last five years, from 2018 to 2023, and written in English. Literature references are only taken from research journals or complete articles that are not a preview of a particular research publication. Several keywords are also used in the process of searching for literature references, so that the references obtained remain focused on the research topic. Keywords to expand search results are a combination of the following words with the Boolean operators: (“electronic payment” OR "e-payment" OR “digital payment” OR “e-wallet” OR “electronic wallet” OR “online transaction” OR “online transactions” OR “mobile payment” OR “m-payment” OR “cashless” OR “cashless transaction” OR “payment gateway”) AND (“security” OR “secure” OR “efficient” OR “securing” OR “risk” OR “risks” OR “fraud” OR “issues”).

Using these keywords, 89 article research were found, which were re-evaluated to maintain the best accuracy, relevance, and credibility. The obtained literature was then applied with inclusion and exclusion criteria, as described in Table 1. These criteria analyzed the quality, suitability, and relevance of the research articles to the research topic based on the alignment of titles and abstracts. These criteria filtered out which research articles would proceed to the next stage and identified articles that were clearly irrelevant to the research topic. The research articles that met the inclusion criteria were included, while those that met the exclusion criteria were not included in this research.

Fifty-six research articles were found once the inclusion criteria were applied. The inclusion and exclusion criteria for the final quality assessment are also applied in the second step. At this point, the literature's content is used to review the quality assessment. The selected articles must be validated for their relevance to the research topic. This process resulted in 34 selected research articles. Figure 2 displays the number of articles chosen according to their publication year, while Table 2 provides a list of these selected articles.

Table 1. Inclusion and Exclusion Criteria

Criteria	Description
Inclusion	Research article is indexed by Google Scholar. Research article discusses e-payment and e-payment security. Research article was published in the period 2018-2023. Research article is written in English.
Exclusion	Research article does not discuss e-payment and e-payment security. Research article is a literature review.

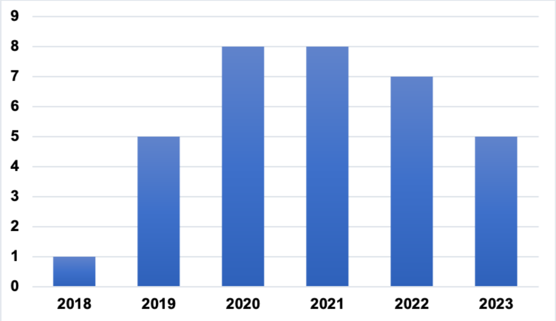

Figure 2. Number of selected research papers based on year of publication

Table 2. List of Selected Papers

No	Year	Country	Title	Authors
1	2018	Korea	Mobile payment in Fintech environment: trends, security challenges, and services	Jungho Kang
2	2019	China	E-commerce Trade Consumption Payment Security and Privacy Based on Improved B2C Model	Linzhu Hu
3	2019	India	Ecommerce Transactions: Secure Gateway in Payment System	Jaiganesh Kalbande
4	2019	Myanmar	Design and Implementation of Electronic Payment Gateway for Secure Online Payment System	Kyaw Zay Oo
5	2019	India	Survey on Online Electronic Payments Security	Sameer Saxena, Sonali Vyas, B. Suresh Kumare, Shaurya Gupta
6	2019	UAE	An Innovative Study of E-Payment Systems Adoption in Higher Education: Theoretical Constructs and Empirical Analysis	Said A. Salloumn, Mostafa Al-Emran, Rifat Khalaf, Mohammed Habes, Khaled Shaalan
7	2020	Malaysia	An Efficient Secure Electronic Payment System for E-Commerce	Md Arif Hassan, Zarina Shukur, Mohammad Kamrul Hasan
8	2020	Egypt	E-Payment Risks, Opportunities, and Challenges for Improved Results in E-Business	Mohmed Hassan Nasr, Mohamed Farrag, Mona Mohamed Nasr
9	2020	China	A Secured Architecture for Transactions in Micro E-Commerce using QR scan, eWallet Payment Applications with Adaptation of Blockchain	Ali Waqas, Md. Hassam Yousaf, Saima Siraj, Usman Ahmed, Vidyasagar S.D., Hemant J. Shinde, Addepalli Lavanya
10	2020	Jordan	Proposed E-payment Process Model to Enhance Quality of Service through Maintaining the Trust of Availability	Khaled AL-Qawasmi, Mohammaf AL-Mousa, Mohammad Yousef
11	2020	Iraq	Secured e-payment system based on automated authentication data and iterated salted hash algorithm	Ali Al Farawn, Hasanein D. Rjeib, Nabeel Salih Ali, Basheer Al-Sadawi
12	2020	China	Electronic Payment Schemes Based on Blockchain in VANETs	Xinyang Deng, Tianhan Gao
13	2020	India	Integration of Biometric Security System to Improve the Protection of Digital Wallet	Ankur Gupta, Dushyant Kaushik, Swati Gupta
14	2020	Bangladesh	Security Aspects of e-Payment System and Improper Access Control in Microtransactions	Md Asaduzzaman
15	2021	USA	Electronic Payment Systems – Payment Gateways and Data Security Standards	Lorraine Jonassen, Binh Tran, Hyesung Park, Karen Benson
16	2021	Malaysia	Device Identity-Based User Authentication on Electronic Payment System for Secure E-Wallet Apps	Md Arif Hassan, Zarina Shukur
17	2021	India	Secured and Efficient Payment Gateways for eCommerce	Jay Patel
18	2021	India	Security Issues and Solutions in E-Payment Systems	Amitesh Yadu, Dr. Vaibhav Sharma
19	2021	Turkey	Blockchain-Based Secure Credit Card Storage System for E-Commerce	Ahmet Ali Süzen, Burhan Duman

20	2021	India	BioPay: A Secure Payment Gateway through Biometrics	Gurpreet Singh, Divyanshi Kaushik, Hritik Handa, Gagandeep Kaur, Sunil Kumar Chawla, Ahmed A. Elngar
21	2021	Uzbekistan	Application of Secure Electronic Transaction Protocol in Electronic Payment System	Shonazarov Soatmurot Qulmurodovich, Bozorov Asqar Khaitmurotovich, Xolliyev Faxriddin Boxodirovich
22	2021	Iraq	Software engineering based secured E-payment system	Muayad Sadik Croock, Rawan Ali Taaban
23	2022	Saudi Arabia	Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in Saudi Arabia	Mohammed Amin Almaiah, Ali Al-Rahmi, Fahad Alturise, Lamia Hassan, Abdalwali Lutfi, Mahmaod Alrawad, Salem Alkhalaf, Waleed Mugahed Al-Rahmi, Saleh Al-sharaieh, Theyazn H. H. Aldhyani
24	2022	USA	Identification of Fraudulent Online Transactions and Protection: State-of-art Techniques	Akshat Gaurav, Brij B. Gupta
25	2022	Bangladesh	Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems	Iffath Tanjim Moon, Muhammad Shamsuzzaman, Muhammad Musfiqur Rahman Mridha, Abu Sayed Md. Mostafizur Rahaman
26	2022	Malaysia	Customer Satisfaction with Digital Wallet Services: An Analysis of Security Factors	Dewan Ahmed Muhtasim, Siok Yee Tan, Md Arif Hassan, Monirul Islam Pavel, Samiha Susmit
27	2022	China	Risk Prediction of E-Payment by Big Data Management Technology	Fei Liu
28	2022	Egypt	A Proposed Fraud Detection Model based on e-Payments Attributes a Case Study in Egyptian e-Payment Gateway	Mohamed Hassan Nasr, Mona Mohamed Nasr, Mohamed Hassan Farrag
29	2022	Korea	E-commerce payment model using blockchain	Shee-Ihn Kim, Seung-Hee Kim
30	2023	USA	Secure Mobile Payment Architecture Enabling Multi-factor Authentication	Hosan Alamleh, Ali Abdullah S. AlQahtani, Baker Al Smadi
31	2023	Malaysia	Use of E-Wallet and Security of Digital Transactions	Azrul Enuar Bin Samsudin, Mohd Khairudin Bin Kasiran
32	2023	India	Fintech innovations in E-payments: Privacy and security in cybercrime threats	K. P. Ramesha, R. Amudhab, K. Prasobc, K. S. Kannad
33	2023	India	Digital Payment Methods: Challenges And Opportunities	Aathira S Nair, Dr .P. Kannan
34	2023	Turkey	Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms	Can Iscan, Osman Kumas, Fatma Patlar Akbulut, Akhan Akbulut

Based on the third stage of the Kitchenham method, the selected research articles will be synthesized and analyzed to answer the research questions. In this stage, relevant information from selected research articles will be extracted to aim the main findings, conclusions, and recommendations regarding the security of electronic payments and provide a comprehensive understanding of this topic. This stage will be discussed in the Results and Discussion section.

RESULT AND DISCUSSION

In this stage, we extracted data from the selected research articles to delve into the findings and answer the research questions.

A. Result

Electronic payments transfer monetary value involving a set of transfer systems in the form of technology and information, especially internet infrastructure that enable the transfer of funds electronically [2], [13]. E-payment can also be made on e-commerce platforms, where exchanging goods for money online and involves electronic transactions as a payment method [14]. Several electronic payment methods were identified, such as Financial Technology (Fintech) Payment, Mobile Payment, Credit Card, Debit Card, Electronic-Wallet (E-Wallet) / Electronic-Cash (E-Cash, mobile or electronic banking (m-banking or e-banking), Smart Cards, and Stored Value Card [3], [15], [16], [17], [18].

Mobile banking and e-banking are defined as the implementation of mobile financial services authorized by financial institutions, including banks, to conduct transactions without the need to go directly to the bank or ATM [3]. These methods of transactions can be made directly via mobile devices, such as smartphones, without the need to use cash or physical cards [17].

Fintech Payment is a third-party service providing digital payment transactions [17]. In contrast to mobile payments which are usually developed and managed by financial institutions, fintech payments are developed by technology companies, hardware manufacturers, and usually collaborate with financial institutions. They work together to provide electronic payment services more simply and efficiently via mobile devices [17].

An e-wallet is an electronic application on a mobile device that collects user data authenticity information with bank data, such as credit card or debit card. Then, the card data can be used to fill the e-wallet with cash and can be used for transactions [3], [18]. Its primary purpose is to facilitate secure electronic transactions. Using an e-wallet, individuals can conveniently make online purchases, transfer funds to other users, settle bills, and engage in various financial transactions using their computer or mobile device [6].

Financial institutions and fintech companies often use payment gateways in developing their electronic payment systems. Payment Gateway (PG) acts as an intermediary server between bank servers, merchants and users in electronic payments. PG is responsible for securing all sensitive information during the transaction process using various security protocols and encryption techniques [18].

There are several fundamental principles regarding electronic payment security mentioned in article references, as shown in Table 3. Authentication refers to verifying user authenticity and ensuring authorized users carry out transactions and have access rights based on password verification, biometric data, or cryptographic techniques [9]. Authentication methods such as PINs, passwords, biometrics, and location-based authentication have been utilized to verify the legitimacy of users during transactions [4]. Unauthorized access is greatly decreased by implementing authentication systems, especially those that use biometrics and multi-factor authentication (MFA). Through the use of one or more authentication methods, these systems guarantee that sensitive payment functions are only accessible to authorized users.

User trust and confidence in electronic payment systems can also be increased by putting strong authentication procedures in place. However, complex authentication procedures may cause user distress in addition to boosting security. Excessively rigid authentication requirements have the potential to irritate users and discourage them from completing transactions.

Table 3. Electronic Payment Principles

Principles	List of Papers	Total
Authentication	[2], [3], [4], [6], [7], [8], [13], [14], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31]	24
Integrity	[2], [3], [8], [13], [14], [15], [16], [17], [21], [22], [23], [32], [33]	13
Privacy	[2], [6], [7], [15], [17], [18], [20], [22], [23], [27], [31], [32]	12
Confidentiality	[2], [3], [7], [8], [13], [14], [15], [16], [18], [19], [20]	11
Non-Repudiation	[2], [3], [13], [14], [15], [16], [20], [21], [22], [23]	10
Availability	[2], [3], [8], [14], [15], [17], [20], [32], [33]	9
Authorization	[6], [8], [14], [17], [21], [24], [25]	7
Vulnerability	[15], [26], [33]	3
Hostility	[15], [20]	2
Atomicity	[17]	1

For payment system providers, the creation, integration, and upkeep of sophisticated authentication methods can be expensive. These expenses could result in lower investments in other areas or be passed on to customers. Recently, dependence on digital wallets has created new challenges in authentication methods. Biometric authentication is often utilized in electronic payments to offer convenience to users. However, this also needs to be accompanied by the security and privacy of biometric data. The increasing variety of Internet of Things (IoT) devices also opens up opportunities for biometric authentication innovation, including iris recognition as a biometric authentication technique [34].

Integrity refers to the complete authenticity of the transactions' data to ensure that payment data is not manipulated illegally during the payment process. Integrity also includes the authorization validity and user identity used in transactions [17]. Prioritizing integrity in the electronic payment system, ensuring transaction data is not changed during transmission, and maintaining the accuracy and reliability of financial records can increase user trust. However, checking transaction integrity can also cause latency problems, such as cryptographic processing of transaction data, which can make transaction processing times slower. As a qualification in fulfilling the integrity aspect, ensuring that transaction or user data has adequate security measures, one of which is cryptographic protocols or the use of artificial intelligence to detect real-time fraud.

Privacy in this context refers to protecting payment information or user transaction patterns in electronic payments using encryption. It is important for electronic payment systems to protect user privacy from criminal attacks and to avoid financial losses for users [17]. Confidentiality protects valuable information from unauthorized access by unauthorized parties. Users' data should only be accessed by authorized parties if it is needed to track it [15]. The implementation of the privacy and confidentiality principles is to ensuring user or transaction data are protected from identity theft and phishing attacks. Implementing this principle is also related to compliance with government regulations, where each country has its own regulations, so this also can be a challenge. Implementing security protocols to protect user data and transactions can also make system design complicated. Therefore, it is crucial to find a balance between ease of access by users and applying privacy and confidentiality in electronic payment systems.

Availability is a state where users can access and use an electronic payment system without significant obstacles or disruptions [17]. Ensuring the availability of electronic payment services is crucial for user satisfaction and trust, as it guarantees continuous service delivery and resilience against attacks. However, achieving high availability often requires costly redundant systems and infrastructure. Maintenance challenges also arise, necessitating constant monitoring and updates to keep systems highly available.

Non-repudiation refers to the ability or preventive action to prevent parties involved in electronic transactions from denying or rejecting responsibility for the actions taken. This mitigation step can be carried out by using digital signatures or certificates to protect all parties against the possibility of rejecting successful transactions [13]. Non-repudiation provides a way to convincingly prove participation in transactions, thereby facilitating dispute resolution and enhancing security. However, implementing non-repudiation mechanisms such as digital signatures will increase the complexity of the system. Storing and managing non-repudiation evidence can raise privacy concerns if not handled properly.

Authorization is validating the authenticity of data and user access rights, ensuring that the user is authorized to carry out certain transactions or actions [13]. Elements confirmed in the authorization process are verification of user identity, validity of the payment method used, and the availability of sufficient funds when the transaction is carried out [17]. Although authentication and authorization are interconnected, they have their respective functions in electronic payments. While authentication verifies the validity of user data accessing the system [9], authorization is carried out after the authentication process. Authorization determines the rights or permission the user has within a system. Treating these two processes as distinct functions allows for a more effective implementation of security measures in electronic payment systems. Authorization systems offer several advantages in electronic payment platforms. By designating permissions at some levels, where users only access features and information pertinent to their roles or transaction requirements, it enhances security and user experience. Additionally, well-defined authorization mechanisms aid in meeting regulatory compliance requirements and streamlining auditing processes. It establishes a clear framework for tracking actions, attributing them to specific users, and determining the authority under which they were performed.

However, there are notable challenges associated with authorization systems. As electronic payment systems expand in scale, managing authorization policies can become increasingly complex. This complexity demands sophisticated tools and expertise, which can add to operational overheads. The potential for misconfiguration also poses a significant risk, potentially leading to vulnerabilities such as unauthorized access to sensitive functions or data. Despite the importance of accurate authorization configurations, ensuring their precision remains challenging.

Vulnerabilities in user data or information breached and misused by unauthorized parties are considered imperfections in electronic payment systems. When exposed data is misused, it can be referred to as an abuse of system security [15]. Vulnerability management includes proactive threat detection and rapid remediation to enhance the security of electronic payment systems. Yet, remediating security vulnerabilities requires significant resources and can produce false positives, leading to unnecessary work and distraction from real threats.

Hostility refers to user trust in making electronic payment transactions, so that during the process, electronic payment service providers can carry out regular testing [15]. User confidence in payment platform security is increased through routine testing and system hardening against hostile acts, which also aid in adapting to new threats. Aggressive hostility testing, like penetration testing, however, can cost a lot of time and money if not handled appropriately and run the risk of disrupting services.

Atomicity refers to transactions with only a single result: failure or success. If there are several operational steps in the transaction process, all of these steps must be declared completed if the transaction is declared successful. On the other hand, if one of these steps fails for any factor or reason, then the transaction must be declared a complete failure [17]. By assuring that transactions are either fully completed or fully reversed, atomicity lowers the possibility of mistakes and inconsistencies, and ensures transaction reliability. Nonetheless, maintaining atomicity increases transaction management complexity and may impose performance costs, which could slow down transaction processing. These principles are related to each other to ensure that all transactions are secure, reliable, and protected from all vulnerabilities.

B. Threats and Vulnerabilities

Despite the continuous development of electronic payment security is ongoing, it still cannot be fully shielded from threats and vulnerabilities. There are numerous factors contributing to risks in electronic payments.

The increasing use of online transactions expands cyber threats to vulnerabilities in electronic payment systems. Vulnerability is a system, software, or infrastructure weakness that unauthorized parties can misuse. Cyberattacks such as unauthorized access theft, data damage, and so on can occur.

Based on 34 selected articles from the 2018-2023 period, the vulnerabilities and threats that have been identified in electronic payment systems are classified into 7 categories. Each category was peer-reviewed by members of the research team. Differences or overlaps between categories are discussed and resolved through consensus, ensuring each category represents distinct threats and vulnerabilities within electronic payment systems. Table 4 described the threat and vulnerability categories in electronic payments.

Table 4. Threats and Vulnerabilities Categories in Electronic Payment

No	Threats and Vulnerabilities	List of Papers	Total
1	Data and Security Breaches:		
	- Data	[7], [8], [15], [18], [23], [24], [27], [29], [31], [32], [33], [34], [35]	21
	- Security	[4], [14], [16], [23], [24], [26], [30], [35]	
2	Lack of Robust Principles	[2], [4], [6], [7], [16], [18], [20], [26], [28], [33], [36], [37], [38]	13
3	Cybersecurity Threats	[3], [8], [15], [25], [31], [33], [39]	7
4	Regulatory Compliance	[33], [38]	2
5	Insider Threats	[6], [29]	2
6	Fraudulent Transactions	[9]	1
7	Lack of Awareness	[16]	1

Data and security breaches ranked first as a threat in electronic payments, mentioned by 21 articles. Data breaches in electronic payment are a massive threat, impacting users and companies. These breaches usually happen because cyber-attacks find and exploit the weak spots in systems to grab sensitive data [8], [23]. The impact of data breaches isn't just about losing data or fraud [24], it's also the loss of customers' trust, potentially causing a hit to a company's reputation that can linger for ages [7], [35]. Data breaches in electronic payments can occur through cybercrime such as phishing, ransomware, IoT security issues, cyber espionage, and DDoS attacks [15], [32], [33]. This can also happen due to a lack of security in information access, thus allowing unauthorized access to occur during transactions [18], [24], [27], [33]. These data breaches can also occur due to malicious software installation [31], social engineering attack [32], or even internal threats when data is misused during the application development process or compromising the operating system's execution [29] and dishonest providers or merchants [6]. Something as simple as losing a mobile device can also jeopardize personal and financial information [34]. While data breaches focus on data loss, security breaches focus on systematic vulnerabilities that allow unauthorized access. This can make users vulnerable to data theft and fraud [4]. Dependence on electronic payment access with payment tools such as credit cards also increases the vulnerability to security threats [14], [30]. Unauthorized access to security breaches allows attackers to exploit the system by bypassing security mechanisms designed to restrict unauthorized access [26]. Within electronic payment systems, there are benefits and drawbacks related to data and security breaches. Positively, security technology improvements offer stronger defenses against breaches, particularly for widely used payment methods like credit/debit cards and e-wallets. Frequent patches and upgrades are essential for successfully reducing these risks and enhancing system security as a whole. But the variety of payment options creates new risks as well. Cybercriminals continually develop innovative methods and exploit these vulnerabilities, requiring constant vigilance and adjustments to security measures. New technologies, such as cryptocurrencies, require constant attention to detail and customization. Often, the frequency and complexity of attacks far outpace the rate of security updates, leaving systems vulnerable to exploitation. While security technologies offer improved defenses, the evolving payments landscape poses ongoing challenges that require proactive measures to address effectively.

The lack of robust principles delves into the fundamental weaknesses within electronic payment systems, as listed in the previous section in Table 3. This shows deficiencies from a technical and organizational perspective, such as poorly designed systems, poor system implementation, and lack of standards of operational guidelines. The absence of this principle in building electronic payments opens up opportunities for threats and weakens the system's resilience, which is also related to moral hazards [38]. Principles such as the availability of electronic payment systems are essential for maintaining user trust and reliability when making transactions and ensuring good service quality [2]. Poor quality systems, such as glitches and bugs, are also considered threats [7], [33]. In electronic payments using physical cards (with magnetic strips or chips), there is also a lack of authentication methods because it depends entirely on whether the user is able to show the card he will use rather than using what only the user knows, such as a PIN or biometric verification [4], [28]. To minimize threats and risks due to the lack of robust principles, this can be mitigated by implementing a payment system compliance with international security standards such as PCI-DSS, which provides a structured approach to maintaining strong security principles. Regular audits are also recommended to ensure compliance and increase the effectiveness of security measures. The dynamic nature of digital payments requires a regular review of implemented principles, which poses challenges for emerging platforms. While established systems benefit from structured security approaches, emerging platforms require adaptation continuously to maintain strong security measures.

Most cyber-attacks aim to exploit financial credentials and user information data [15]. Cybersecurity threats include malicious activities targeting electronic payment systems, including deceptive calls pretending to be from electronic payment companies to phis for account details [39]. Cyber threats are changing rapidly, forcing defense strategies for electronic payment security systems to continue to be developed. Cybercrime threats, such as man-in-the-middle attacks, code injection, and zero-day exploits, can compromise authentication, integrity, and availability in electronic payments [3]. The significance of compliance in ensuring that payment systems adhere to legal standards and best practices cannot be overstated [38]. It plays a crucial role in safeguarding consumers and preserving the integrity of the financial ecosystem.

Compliance with these standards by developing and implementing robust risk control systems [38] and compliance with a regulatory framework [33] could prevent financial fraud and data breaches and build consumer trust in payment systems. It involves a comprehensive approach that encompasses not just adherence to regulations but also the adoption of best practices in security and operational procedures. By maintaining a high level of compliance, payment systems demonstrate their commitment to consumer protection and the financial system's stability. Many electronic payment platforms also open up opportunities for threats, including fraudulent transactions. Many transaction platforms are closely related to security breaches and cybersecurity threats, including exploiting system vulnerabilities or tricking users to gain access. In this case, the threat is in the form of fraud that resembles legitimate transactions [9].

Even though all threats and vulnerabilities have been identified and security defense methods continue to be developed, it does not rule out the possibility that there will still be vulnerabilities in electronic payment transactions caused by human factors. Lack of awareness in this context points towards a different knowledge and confidence among users about the mechanisms and protection in electronic transactions. When the response to an electronic payment does not match what it should be, the lack of user awareness causes the user's response to refuse to use it or even opens up the opportunity to be tricked by irresponsible parties [16]. Nowadays, campaigns for continuous education and awareness are now more focused and successful, reaching a larger audience through the use of social media and other channels. By taking this proactive stance, users—especially those utilizing widely used payment systems—are better equipped to identify fraud and defend against certain dangers. The rapid development of new payment methods, however, presents difficulties. Users who need to be made aware of this new technology, particularly those who are less tech-savvy, may be open to exploitation. The incidence and sophistication of fraud continue to rise in spite of educational initiatives, frequently surpassing the impact of awareness campaigns. This emphasizes the necessity of continual learning and adjustment to stay up to date with advancements in cybersecurity risks and electronic payment systems.

C. Security Methods

Facing various threats in electronic payments, numerous preventive actions have been implemented to continue enhancing the security of electronic payments. From the selected references, security methods are divided into several categories, as described in Table 5. A diverse range of security methods has been developed and implemented, and these methods are pivotal in mitigating vulnerabilities and ensuring the robustness of electronic payments.

Authentication and Authorization Systems, including techniques such as biometric verification, live location tracking, device identity validation, and automated authentication processes, are crucial. These methods, as referenced in 9 papers, provide a foundational layer of security by ensuring that only legitimate users can access and initiate transactions. Alamleh *et al.* emphasize multi-factor authentication as a guarantor of the validity of transactions and propose a mobile payment architecture that utilizes the security features of modern smartphones as a fraud prevention measure [4].

Table 5. Security Methods in Electronic Payment

No	Security Methods	List of Papers	Total
1	Authentication and Authorization System (Biometric, Live Location, Device-Identity, Automated Authentication)	[4], [15], [28], [29], [30], [33], [34], [37]	9
2	Encryption, Cryptography, and Secure Communication Protocols	[2], [3], [4], [7], [8], [14], [14], [16], [17], [18], [19], [23], [24], [25], [27], [31], [33], [33], [37]	18
5	Access Control and Key Management	[26], [36]	2
3	Fraud Detection and Risk Management	[4], [33], [38], [39]	4
4	Artificial Intelligence and Blockchain Payment Schemes	[2], [6], [9], [20], [21], [23], [31], [32], [38], [39]	10

Several verification methods are used in this payment architecture, such as verification of funds availability, biometric verification such as fingerprints and FaceID, and location verification [4], [30], [29]. An authentication system using iris-based biometrics has also been proposed, integrating canny-based edge detection to reduce biometric model space consumption. By using a complex iris pattern, the authentication process can be safer and more secure [34]. The others also discussed the authentication mechanism using the International Mobile Equipment Identity (IMEI) of the mobile device used by the user [28] and using RFID technology along with an iterated salted hash algorithm for password encryption [37]. Biometrics, one-time passwords, and face recognition are not only used in the authentication process but also in authorizing transactions [28]. In addition, Kang emphasized the importance of building secure and user-friendly mobile payment solutions that can authenticate both parties, ensure the integrity and privacy of transactions, provide reliable and uninterrupted service, and handle transactions completely or not at all to prevent partial processing issues [17]. Nowadays, biometrics is frequently employed as a method of authorization and authentication, representing a secure and convenient verification procedure for electronic payments. However, the current utilization of biometrics also brings up new challenges, particularly with regard to the processing and storage of biometric data. The use of these technologies has been impacted, for instance, by stricter consent and data handling regulations resulting from revisions to the General Data Protection Regulation (GDPR) in Europe [40].

Encryption and Cryptography are also cited in 18 papers, highlighting their critical role in safeguarding data integrity and confidentiality. These methods use complex algorithms to encode information, making it accessible only to those with the correct decryption keys, thus protecting sensitive data from unauthorized access or tampering. The Secure Electronic Transaction (SET) protocol which is similar to the 3D Secure protocols by Visa and MasterCard, is also used for encryption [18]. SET's primary aim is to safeguard the cardholder's payment information. It uses a combination of encryption and digital signature technologies to provide a secure and private communication channel between all parties involved in a transaction: the cardholder, the merchant, and their respective banks. This protocol is achieved by encrypting the payment details in such a way that only the cardholder's bank can decrypt and process them. Meanwhile, digital signatures verify the authenticity of the transaction, confirming that the messages have not been altered in transit and that they come from a legitimate source [18]. Unfortunately, this protocol was not widely adopted and was eventually overtaken by simpler protocols such as SSL/TLS [7], [18].

The Secure Socket Layer (SSL) protocol secures data transmission, minimizes the time required for encryption and decryption, and protects payment details by setting standards to create a secure connection between a browser and a web server [7], [27]. This protocol functions through a cryptographic mechanism employing two keys for data encryption: a public key accessible to all and a private or secret key exclusive to the message's recipient. It guarantees that all information exchanged between the web server and browsers stays confidential and integral [7], [27]. In current conditions, SSL has been considered to be replaced by Transport Layer Security (TLS). TLS is an evolution of SSL that supports more robust encryption [8]. However, SSL and TLS are still often associated with a security context for data transportation over the internet, so many people refer to them as SSL/TLS.

Jay Patel mentions how payment gateway has an important role in maintaining payment security in India, from customers placing orders, filling in payment details, to transaction authorization and payment completion [7]. However, using a payment gateway is considered to have several weaknesses, such as: the possibility of leaking personal information, technical problems, or user inconvenience in using web-based payment applications. The choice of using a payment gateway as an electronic payment service must be made by considering several parameters and features, including security, compliance with PCI-DSS standards and using SSL/TLS for data encryption [7].

Kway Zay Oo proposed a method that transmits payment data, such as credit or debit card data, directly to a payment gateway without going through merchants [8]. In this method, the SSL with Rivest-Shamir-Adleman (RSA) algorithm is utilized to enhance security in the payment process. This method can provide confidentiality by using RSA to act as an intermediary to complete transactions between online merchants and customers. RSA was chosen due to its large prime numbers and key sizes, enhancing security. However, the RSA algorithm used in this proposed method only generates keys with a size of 256-2096 bits and can’t encrypt keys with a size larger than that [8].

Furthermore, using the Triple Data Encryption Standard (TDES) and RSA Cryptosystem within a payment gateway also accelerates the transaction process without compromising its security [14]. TDES applies encryption three times to data blocks, making it highly resistant to attacks. At the same time, the RSA Cryptosystem uses a pair of keys, public and private, for encryption and decryption, ensuring that only intended recipients can access the data [14]. Even though it still has potential weaknesses, the ability of payment gateways to adapt to the digital payment landscape has increased its capacity, especially in accommodating various electronic payment methods, including e-wallets and emerging digital currencies. This makes payment gateways an option as a security method for electronic payments.

Access Control and Key Management, mentioned in 2 papers, are essential for defining and enforcing who has access to specific data and systems within electronic payment environments, further securing payment processes against unauthorized access and ensuring data privacy. It also plays a crucial role in safeguarding e-payment infrastructure from cyberattacks, as it prevents attackers from manipulating systems for monetary gain by bypassing security measures designed to block unauthorized access to system assets [25], [33]. To tackle these security hurdles, the document highlights the necessity of strong access control systems, consistent vulnerability evaluations, and the application of security best practices throughout the entire electronic payment ecosystem, encompassing customers, vendors, payment service providers (PSPs), and bank servers [26]. Croock and Taaban mention a software engineering technique with a back-propagation algorithm on a neural network to ensure the security level of the generated key, with a random level of master key and session key used to authenticate user devices in mobile applications [36]. In most-recent consideration, the widespread adoption of cloud-based infrastructure and services has drawn attention to the importance of reliable key management and access control systems that can function well in decentralized environments. Reducing trust assumptions and adopting zero-trust architectures are emerging trends in addressing access management challenges in highly scalable and dynamic cloud environments [41].

Fraud Detection and Risk Management strategies, discussed in 4 papers, employ analytical tools and monitoring systems to identify and mitigate potential threats and anomalous activities, thereby reducing the risk of fraudulent transactions. Alamleh *et al.* emphasize multi-factor authentication as a guarantor of the validity of transactions and propose a mobile payment architecture that utilizes the security features of modern smartphones as a fraud prevention measure [4]. Fraud detection can be done using machine learning algorithm methods such as decision tree algorithms and Hidden Markov Models (HMM) to analyze user behaviour or patterns [6], [39]. However, some machine learning methods require a high computing system, so the costs incurred can be quite significant.

This fraud detection and risk management also led to Artificial Intelligence and Blockchain Payment Schemes, explored in 10 papers. Uses of big data management technology and BP neural networks to predict the risks of electronic payment systems [9], [38]. This approach involves analyzing extensive e-payment data to identify potential risks, thereby improving the security and reliability of e-payment systems through advanced data analysis and prediction techniques [38]. Blockchain technology utilizing AES 256 bits encryption and SHA256 data integrity is used to store credit card information data in e-commerce applications securely [23]. Blockchain-based electronic payment schemes in Vehicular Ad-hoc Networks (VANETs) can also improve transaction efficiency and security [20]. Apart from security, the blockchain model in payment transactions in e-commerce is also considered to be able to reduce transaction costs [21], such as the application of architecture for micro e-commerce using a QR scan-based payment application with an adaptation of blockchain technology [31]. Integrating AI and blockchain in risk management strategies provides promising opportunities to improve electronic payment systems' security and efficiency. Although using AI advanced fraud detection algorithms increases anomaly detection accuracy, the accompanying expenses must be considered. However, implementing blockchain technology has the added benefit of lower costs and increased security.

All these findings not only contribute to the theoretical understanding of electronic payment security but also have significant practical implications. By integrating blockchain technology, for example, electronic payment systems can achieve unprecedented levels of transaction integrity and transparency, reducing the risk of fraud and increasing user trust. Together, these security methods form a comprehensive security framework for electronic payment systems, addressing a wide range of potential vulnerabilities and threats. The diversified approach, integrating traditional security mechanisms with innovative technologies, underscores the dynamic and evolving nature of electronic payment security.

CONCLUSION

In contrast to previous research which tended to focus on one particular geographic or technological context, this research adopts a global and multi-technology approach, providing new insights into how various security solutions can be applied universally to improve security in electronic payments. This research examines various threats and security to electronic payment systems. This report describes a number of possible threats and the security measures required to mitigate these threats. Through a detailed analysis of the existing literature, it is firmly established that the integrity, confidentiality, availability, authenticity and authorization of electronic payment systems are of paramount importance. Technological advances and cyber threats have ushered in a new era where electronic payment security is under constant siege, highlighting the importance of an adaptable and robust security framework.

In the digital era, electronic payment systems have become the backbone of financial transactions, offering unprecedented convenience and efficiency. However, this evolution is accompanied by a growing number of security threats that pose significant risks to the integrity and confidentiality of these systems. This study carefully addresses two important existing research questions on electronic payment security: identification of common threats and exploration of robust security measures to counter these threats.

The threats identified in this research cover a spectrum of vulnerabilities, from data and security breaches to violating strong principles and the emerging danger of cyberattacks. Data breaches stemming from sophisticated phishing, ransomware and DDoS attacks highlight the vulnerability of electronic payment systems to unauthorized access and unauthorized seizure of sensitive data. Uncovering these breaches not only results in financial losses and erodes consumer trust but also has the potential to harm the reputation of the entities involved. Additionally, disregard for basic security principles and the relentless evolution of cyber threats emphasize the need for a dynamic and comprehensive approach to protecting electronic payment systems.

Addressing these difficult challenges, this research has identified and recommended a set of security measures designed to fortify electronic payment systems against identified threats, such as implementing advanced authentication and authorization systems, including biometric verification and multi-factor authentication, which work to verify user identity with a high degree of accuracy. Encryption and cryptography have emerged as indispensable tools for ensuring the confidentiality and integrity of transaction data, effectively protecting it from unauthorized interception and manipulation. Additionally, the integration of blockchain technology offers a revolutionary approach to securing transactions through a decentralized and immutable ledger, providing strong protection against fraud and unauthorized access.

In conclusion, this research emphasizes the importance of implementing holistic and adaptive security strategies to overcome the complex nature of electronic payment security. The continued evolution of cyber threats requires a dynamic and proactive security approach, integrating cutting-edge technologies and adhering to strict regulatory standards. In order to enhance fraud detection and prevention systems, future research should explore cutting-edge technology like artificial intelligence and quantum computing. In addition, the development of a global context regarding security standards and practices can significantly increase the resilience of electronic payment systems to global threats. The findings of this SLR on threats and security methods within electronic payment systems also provide valuable insights for a range of stakeholders. Financial institutions and payment service providers can evaluate and improve their security measures, thereby building user trust and improving existing frameworks. Regulatory organizations can use this research study to develop new regulations that effectively regulate the latest innovations in electronic payment systems. For technology developers and researchers, this research acts as a roadmap for identifying areas of innovation and addressing gaps in existing research. Additionally, industry associations also play a vital role in promoting collaboration among stakeholders and advocating for the adoption of shared security standards across the electronic payment ecosystem. Protecting the future of electronic transactions demands a collaborative approach among all parties involved, such as regulators, banks, tech companies, and users, to build a secure, reliable, and robust digital finance environment.

REFERENCES

[1] H. N. Wolff, “Indonesia: online transaction value 2022,” Statista. Accessed: Jan. 09, 2024. [Online]. Available: https://www.statista.com/statistics/958171/indonesia-online-transaction-value/

[2] K. AL-Qawasmi, “Proposed E-payment Process Model to Enhance Quality of

Service through Maintaining the Trust of Availability," *IJETER*, vol. 8, no. 6, pp. 2296–2300, Jun. 2020, doi: 10.30534/ijeter/2020/16862020.

[3] I. T. Moon, M. Shamsuzzaman, M. M. R. Mridha, and A. S. Md. M. Rahaman, "Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems," *JCC*, vol. 10, no. 07, pp. 103–129, 2022, doi: 10.4236/jcc.2022.107007.

[4] H. Alamleh, A. A. S. AlQahtani, and B. Al Smadi, "Secure Mobile Payment Architecture Enabling Multi-factor Authentication," in *2023 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, USA: IEEE, Apr. 2023, pp. 19–24. doi: 10.1109/SIEDS58326.2023.10137778.

[5] A. Aptika, "Upaya Kominfo Berantas Aksi Penipuan Transaksi Online," Ditjen Aptika. Accessed: Mar. 03, 2024. [Online]. Available: https://aptika.kominfo.go.id/2022/10/upaya-kominfo-berantas-aksi-penipuan-transaksi-online/

[6] M. Nasr, M. Farrag, and M. Nasr, "E-Payment Risks, Opportunities, and Challenges for Improved Results in E-Business," *IJICIS*, vol. 20, no. 1, pp. 1–20, Jun. 2020, doi: 10.21608/ijicis.2020.31514.1018.

[7] J. Patel, "Secured and Efficient Payment Gateways for eCommerce," *IJRPR*, vol. 2, no. 7, pp. 575–582, 2021.

[8] K. Z. Oo, "Design and Implementation of Electronic Payment Gateway for Secure Online Payment System," *IJTSRD*, vol. 3, no. 5, pp. 1329–1334, Aug. 2019.

[9] A. Gaurav and B. B. Gupta, "Identification of Fraudulent Online Transactions and Protection: State-of-art Techniques," *edeij*, vol. 1, no. 3, p. e07, Nov. 2022, doi: 10.55234/edeij-1-3-07.

[10] N. Parmar and D. S. Machhar, "A STUDY on the ADOPTION of E-PAYMENT SYSTEMS in INDIA: A LITERATURE REVIEW," 2022.

[11] E. Susanto, I. Solikin, and B. S. Purnomo, "A REVIEW OF DIGITAL PAYMENT ADOPTION IN ASIA," *AIJBES*, vol. 4, no. 11, pp. 01–15, Mar. 2022, doi: 10.35631/AIJBES.411001.

[12] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Information and Software Technology*, vol. 55, no. 12, pp. 2049–2075, Dec. 2013, doi: 10.1016/j.infsof.2013.07.010.

[13] L. Jonassen, B. Tran, H. Park, and K. Benson, "Electronic Payment Systems – Payment Gateways and Data Security Standards," *JEP*, vol. 12, no. 3, pp. 185–193, Jan. 2021, doi: 10.7176/JEP/12-3-21.

[14] M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Efficient Secure Electronic Payment System for E-Commerce," *Computers*, vol. 9, no. 3, p. 66, Aug. 2020, doi: 10.3390/computers9030066.

[15] S. Saxena, S. Vyas, B. S. Kumar, and S. Gupta, "Survey on Online Electronic Paymentss Security," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Dubai, United Arab Emirates: IEEE, Feb. 2019, pp. 756–751. doi: 10.1109/AICAI.2019.8701353.

[16] A. Yadu and D. V. Sharma, "Security Issues and Solutions in E-Payment Systems," *IJARCSMS*, vol. 9, no. 7, pp. 9–14, 2021.

[17] J. Kang, "Mobile payment in Fintech environment: trends, security challenges, and services," *Hum. Cent. Comput. Inf. Sci.*, vol. 8, no. 1, p. 32, Dec. 2018, doi: 10.1186/s13673-018-0155-4.

[18] J. Kalbande, "Ecommerce Transactions: Secure Gateway in Payment System," *IRJET*, vol. 06, no. 06, pp. 421–427, 2019.

[19] M. A. Almaiah *et al.*, "Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in Saudi Arabia," *Electronics*, vol. 11, no. 23, p. 3926, Nov. 2022, doi: 10.3390/electronics11233926.

[20] X. Deng and T. Gao, "Electronic Payment Schemes Based on Blockchain in VANETs," *IEEE Access*, vol. 8, pp. 38296–38303, 2020, doi: 10.1109/ACCESS.2020.2974964.

[21] S.-I. Kim and S.-H. Kim, "E-commerce payment model using blockchain," *J Ambient Intell Human Comput*, vol. 13, no. 3, pp. 1673–1685, Mar. 2022, doi: 10.1007/s12652-020-02519-5.

[22] S. A. Salloum, M. Al-Emran, R. Khalaf, M. Habes, and K. Shaalan, "An Innovative Study of E-Payment Systems Adoption in Higher Education: Theoretical Constructs and Empirical Analysis," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 13, no. 06, Art. no. 06, Jun. 2019, doi: 10.3991/ijim.v13i06.9875.

[23] A. A. Süzen and B. Duman, "Blockchain-Based Secure Credit Card Storage System for E-Commerce," *Sakarya University Journal of Computer and Information Sciences*, vol. 4, no. 2, pp. 204–215, Aug. 2021, doi: 10.35377/saucis.04.02.895764.

[24] S. S. Qulmurodovich, B. A. Khaitmurotovich, and X. F. Boxodirovich, “APPLICATION OF SECURE ELECTRONIC TRANSACTION PROTOCOL IN ELECTRONIC PAYMENT SYSTEM,” *Galaxy International Interdisciplinary Research Journal*, vol. 9, no. 6, Art. no. 6, Jun. 2021.

[25] K. P. Ramesh, R. Amudha, K. Prasob, and K. S. Kanna, “Fintech innovations in E-payments: Privacy and security in cybercrime threats,” *Multidisciplinary Science Journal*, vol. 5, pp. 2023ss0320-2023ss0320, Aug. 2023, doi: 10.31893/multiscience.2023ss0320.

[26] M. Asaduzzaman, “Security Aspects of e-Payment System and Improper Access Control in Microtransactions,” Art. no. 3717, Jul. 2020, Accessed: Mar. 04, 2024. [Online]. Available: https://easychair.org/publications/preprint/ZFhp

[27] L. Hu, “E-commerce Trade Consumption Payment Security and Privacy Based on Improved B2C Model,” *IJNS*, vol. 21, no. 4, pp. 545–550, Jul. 2019, doi: 10.6633/IJNS.201907 21(4).02.

[28] M. A. Hassan and Z. Shukur, “Device Identity-Based User Authentication on Electronic Payment System for Secure E-Wallet Apps,” *Electronics*, vol. 11, no. 1, p. 4, Dec. 2021, doi: 10.3390/electronics11010004.

[29] A. E. B. Samsudin and M. K. B. Kasiran, “Use of E-Wallet and Security of Digital Transactions,” *Journal of Information Systems and Digital Technologies*, vol. 5, no. 2, pp. 155–169, 2023.

[30] G. Singh, D. Kaushik, H. Handa, G. Kaur, S. K. Chawla, and A. A. Elngar, “BioPay: A Secure Payment Gateway through Biometrics,” *JCIM*, pp. 65–76, 2021, doi: 10.54216/JCIM.070202.

[31] A. Waqas, Yousaf, S. Siraj, U. Ahmed, H. Shinde, and L. Addepalli, “A Secured Architecture for Transactions in Micro E-Commerce using QR scan, e- Wallet Payment Applications with Adaptation of Blockchain,” *International Journal of Emerging Technologies in Learning (iJET)*, vol. 11, pp. 611–615, Nov. 2020.

[32] C. Iscan, O. Kumas, F. P. Akbulut, and A. Akbulut, “Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms,” *IEEE Access*, vol. 11, pp. 131465–131474, 2023, doi: 10.1109/ACCESS.2023.3321666.

[33] A. S. Nair and D. P. Kannan, “Digital Payment Methods: Challenges And Opportunities,” 2023.

[34] A. Gupta, D. Kaushik, and S. Gupta, “Integration of Biometric Security System to Improve the Protection of Digital Wallet,” *SSRN Journal*, 2020, doi: 10.2139/ssrn.3595302.

[35] D. A. Muhtasim, S. Y. Tan, M. A. Hassan, M. I. Pavel, and S. Susmit, “Customer Satisfaction with Digital Wallet Services: An Analysis of Security Factors,” *IJACSA*, vol. 13, no. 1, 2022, doi: 10.14569/IJACSA.2022.0130124.

[36] M. S. Croock and R. A. Taaban, “Software engineering based secured E-payment system,” *IJECE*, vol. 11, no. 5, p. 4413, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4413-4422.

[37] A. A. Farawn, H. D. Rjeib, N. S. Ali, and B. Al-Sadawi, “Secured e-payment system based on automated authentication data and iterated salted hash algorithm,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 1, Art. no. 1, Feb. 2020.

[38] F. Liu, “Risk Prediction of E-Payment by Big Data Management Technology,” *Mathematical Problems in Engineering*, vol. 2022, pp. 1–8, Jun. 2022, doi: 10.1155/2022/6815255.

[39] M. H. Nasr, M. H. Farrag, and M. M. Nasr, “A Proposed Fraud Detection Model based on e-Payments Attributes a Case Study in Egyptian e-Payment Gateway,” *IJACSA*, vol. 13, no. 5, 2022, doi: 10.14569/IJACSA.2022.0130522.

[40] “The general data protection regulation.” Accessed: Apr. 02, 2024. [Online]. Available: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

[41] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, “Survivable zero trust for cloud computing environments,” *Computers & Security*, vol. 110, p. 102419, Nov. 2021, doi: 10.1016/j.cose.2021.102419.