JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 38 (2026) 32-42
Received: 19 September 2025
Accepted: 18 November 2025

# A Review of Security Mechanisms in Electronic Payment Systems

Omniah Abdullah ALibrahim*, Suhair Alshehri

*Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*

**Abstract**
Over the last decade, advances in information technology have driven e-commerce and e-payment, enabling global transactions anytime. While offering convenience, these systems raise concerns because fraud, identity theft, and unauthorized payments continue to grow. This paper examines e-payment security, focusing on transaction and protocol vulnerabilities in encryption, authentication, and data integrity, and explores cryptography, authentication mechanisms, and novel architectures. It stresses balancing security and ease of use. Though newer encryption methods and blockchain enhance security, overhead and scalability remain issues. Secure digital transactions require multi-dimensional architectures that integrate authentication, privacy, integrity, non-repudiation, and traditional cryptography with modern technology.

*Keywords*: E-payment security; secure e-commerce; security methods; payment transaction; payment protocols

*Corresponding author
*Email address*: omohammedtaiebalibrahim@stu.kau.edu.sa

## 1. Introduction

Over the past ten years, electronic payment systems have drawn much interest as potential replacements for conventional payment methods. Due to the slow adoption of this technology, cash payments are still prevalent in many markets and account for up to 90% of typical payments in some developing nations [1]. In the modern world, information and communication technologies are widely employed. Thus, electronic payments are replacing traditional methods that require face-to-face interaction [2]. New methods of making electronic payments, which must be made regardless of the type of device being used, are becoming increasingly common. Examples include Apple Pay, Samsung Pay, and Android Pay. The ability to make payments electronically from any location without being present or exposing one's identity is just one of the many benefits customers can enjoy.

On the other hand, some disadvantages related to security issues, like compromising confidentiality, integrity, and availability [3], lead to money theft on electronic payment cards. Attackers are becoming increasingly attentive to exploiting the vulnerabilities of these applications, which may cause trouble for their users. Notably, there has been a growing number of reports of money theft involving electronic payment cards. This means the recent payment applications still lack crucial information security properties [4].

The design and implementation of a robust electronic payment scheme for safeguarding online transactions over time have received substantial attention due to the rise in the importance of electronic payment security. Rivest put up the first micropayment scheme in 1996 [5]. Due to the benefits of the market for these apps, mobile payment applications have been a significant industry focus today and have quickly entered the mainstream. However, these services come with security risks and user privacy hazards. Potential security threats to existing electronic payment technologies concerning the hardware, software, and communication architectures include misuse of stolen devices, inherent operating systems or payment applications access permission, fraud carried out through phishing and software engineering, compromising cardholders' sensitive data, and different attacks such as man in the middle (MITM) and denial of service (DoS) attacks [6].

The security requirements for each electronic payment system should include authentication, access control, confidentiality, integrity, availability, and non-repudiation. Verifying the user and the data source's origin requires two authentication steps. Authorized users can only access the payment system, while illegitimate users are prevented. During the exchange of data, confidentiality seeks to conceal the information. Integrity makes sure that the data being communicated has not been altered. Non-repudiation guarantees that the specified user delivered the message, and availability guarantees that the system is reachable [7]. The electronic payment will be secure for every party if the transaction involves these services.

The process of electronic payment normally entails some crucial stages that help to ensure that the transaction is made securely and efficiently between the seller, buyer, and the payment gateway (e.g., bank). The process is initiated when a customer chooses goods or services and places an order by way of an online platform. This process involves adding items to a digital shopping cart and going to the checkout point. Upon reaching the checkout point, the shopper is asked to provide payment details that could be credit or debit card details, digital wallet credentials, or alternative payment modes like UPI or net banking. After providing payment details, the payment details are sent by a payment gateway, a bridge between the e-commerce website and the shopper's bank [8]. The payment gateway sends the transaction request to the acquiring bank and the associated card network (like Visa or Mastercard), and this card network contacts the issuing bank to authenticate the shopper's credentials, available balance, and conduct fraud verifications. If the transaction is approved, an authorization message gets communicated back over the same chain, confirming the purchase. Parallel to this, the order gets processed to fulfill the order by digital delivery or shipping [6]. The payment settlement is the last step, where money is transferred by the shopper's bank to the merchant's account. A lot of data is sent and stored by this process at various touchpoints, and hence, security is a vital element. Any vulnerability in this process can lead to data breaches, fraud, or failure to make a transaction, emphasizing the need to have a better understanding of this process to make e-payment security frameworks more robust.

### 1.1. Steps of Standard Electronic Payments

Most basic online payments have an orderly sequence of clearly outlined processes to ensure transactional success and security for all parties.

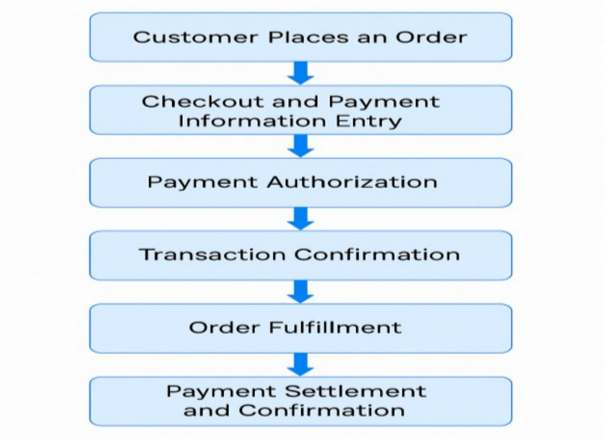

Figure 1: Steps of Standard Online Payments.

1. Customer Submits an Order: The process for online payments starts when an individual chooses an item or service on an online store website and proceeds to make an order. Customers are asked to confirm their choices and enter necessary information, including shipping and any voucher codes.
2. Payment Information Input at Checkout: At this point, the user enters their payment details. This may include typing in debit or credit card details, accessing an electronic wallet such as PayPal or Apple Pay, or utilizing available bank transfer services [9]. The system now proceeds to execute the payment.
3. Authorization for Payment: After the order is confirmed by the customer, the transaction proceeds to authorization for payment. This is when the merchant's payment gateway contacts the payment processor and the issuing bank of the customer. Through secure encryption standards such as SSL, the bank verifies the card details, inspects for sufficient funds, and performs fraud checking. If all is well, the bank approves the payment.
4. Transaction Confirmation: Once authorization is granted, there is an acknowledgment sent back through the bank chain to the payment gateway and the e-commerce platform. Funds are reserved (but not necessarily withdrawn immediately) for the merchant.
5. Order fulfillment: Once payment is secured; the merchant goes ahead to process the order. For digital products, delivery could be immediate, although physical goods are packed and dispatched [10]. A delivery tracking number or timeline is also provided to the buyer at this point, depending on the service type.
6. Payment Settlement and Confirmation: At stage six, settlement is accomplished by the payment processor transferring funds from the buyer's bank to that of the merchant. This process can take from hours to two business days, depending on each bank's processes and the payment method used. A final confirmation is provided to both seller and buyer after the settlement is done.

Each one of these processes is secured through encryption tools, authentication processes, and standards for compliance such as PCI-DSS for protecting sensitive information. Seamless execution by these phases makes both merchant companies as well as customers safe in their use of the digital payments system.

### 1.2. Methodology and Selection Criteria

This review focused on peer-reviewed research published between 2017 and 2024. Relevant studies were identified through major digital libraries, including IEEE Xplore, ScienceDirect, SpringerLink, and MDPI. The inclusion criteria comprise: (1) research addressing security in electronic payment systems, (2) studies proposing or analyzing cryptographic, authentication, or blockchain-based mechanisms used in the payment field, and (3) works including either formal verification or practical evaluation. Non-technical reports, opinion articles, and studies outside the scope of secure payment processing were excluded. A total of 16 papers were selected to ensure both breadth and technical depth of coverage.

To provide a structured overview of the reviewed literature, Figure 2 illustrates the taxonomy of this study, which organizes the research into two primary dimensions aligned with the main sections of the paper: (1) the security of electronic payment transactions, and (2) the security of electronic payment protocols. The first dimension focuses on securing the transaction itself through cryptographic mechanisms, certificateless schemes, and

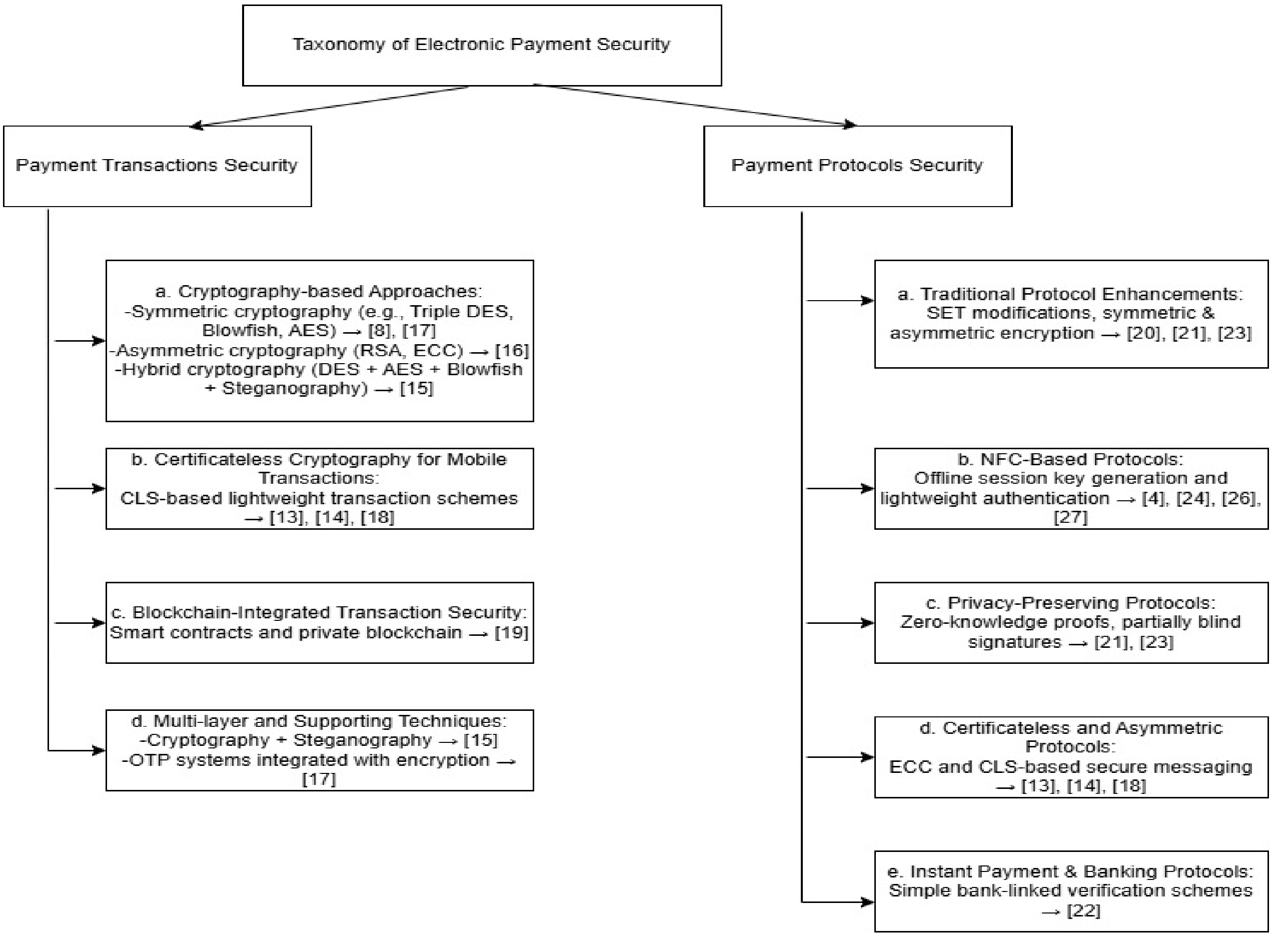
Taxonomy of Electronic Payment Security
Payment Transactions Security
Payment Protocols Security
a. Cryptography-based Approaches: -Symmetric cryptography (e.g., Triple DES, Blowfish, AES) → [8], [17] -Asymmetric cryptography (RSA, ECC) → [16] -Hybrid cryptography (DES + AES + Blowfish + Steganography) → [15]
b. Certificateless Cryptography for Mobile Transactions: CLS-based lightweight transaction schemes → [13], [14], [18]
c. Blockchain-Integrated Transaction Security: Smart contracts and private blockchain → [19]
d. Multi-layer and Supporting Techniques: -Cryptography + Steganography → [15] -OTP systems integrated with encryption → [17]
a. Traditional Protocol Enhancements: SET modifications, symmetric & asymmetric encryption → [20], [21], [23]
b. NFC-Based Protocols: Offline session key generation and lightweight authentication → [4], [24], [26], [27]
c. Privacy-Preserving Protocols: Zero-knowledge proofs, partially blind signatures → [21], [23]
d. Certificateless and Asymmetric Protocols: ECC and CLS-based secure messaging → [13], [14], [18]
e. Instant Payment & Banking Protocols: Simple bank-linked verification schemes → [22]

Figure 2: Taxonomy of Electronic Payment Security.

blockchain integration. The second dimension focuses on protocol-level security measures ensuring trust, authentication, and message integrity between entities. This classification not only aligns with the structure of the review but also highlights underexplored areas such as tokenization-based security and formal verification of protocols.

## 2. The Security of Electronic Payment Transactions

Sensitive data should be safely transmitted between electronic payment parties through the Internet to secure every step of the online transaction. Cryptography is the most effective technique used to secure online transactions from attackers. In addition, it mitigates the Internet communication vulnerabilities such as cross-site snatching [8]. Cryptography plays a vital role in dealing with security features, primarily to authenticate and protect the confidentiality and privacy of sensitive data, so it must be applied at each level of electronic payment transactions. Cryptography is performed as two main processes, encryption and decryption. In the encryption process, the data, known as plaintext, transforms into another form known as ciphertext by using the symmetric or asymmetric key. Decryption is the reverse process of encryption. Symmetric and asymmetric are two different cryptography techniques, as shown in Table 1. To take advantage of both techniques, symmetric encryption can be applied to protect the public key and checksum of the asymmetric method [11].

Table 1: The comparison between symmetric and asymmetric encryption

| Symmetric Encryption | Asymmetric Encryption |
|---|---|
| Consists of one key for encryption and decryption | Consists of two keys, known as the public key and the private key |
| Before starting encryption, two parties should agree upon the same secret key [12] | One public key is available and no need to agree upon secret key [12] |
| Is 100 times faster than asymmetric | Is 100 times slower than symmetric |
| No need for third party | Involves a third party known as a certificate authority |
| Example: RC4, AES, DES, 3DES, Blowfish and Twofish. | Example: RSA, Diffie-Hellman, ECC, DSA, El-Gamal. |

A brief discussion of some research on secure electronic payment transactions is provided. The authors [8] proposed a novel technique to secure e-commerce transactions. The proposed technique is based on the data encryption standard (D.E.S.), which is applied three times for each data block. The significant advantage of triple D.E.S. is the level of security provided, which is billions of times higher than D.E.S. and other frequently used encryption techniques, such as Rivest–Shamir–Adleman (R.S.A.) and a hash function. However, the triple D.E.S. proposed is three times slower than D.E.S., and this technique has issues regarding key sharing. Initially [13], the author demonstrates the difference between certificate and certificateless cryptography. The certificate cryptography is based on traditional public key infrastructure that uses a certification authority to distribute and manage all private and public keys of the system. While certificateless cryptography does not need any certificates to ensure authority. At the same time, certificateless cryptosystems can provide robust security transactions for mobile payment applications. In addition to fulfilling the capability of the IoT network environment, which has constrained resources and limited bandwidth of mobile objects. The proposed C.L.S. scheme for the transaction of mobile payment proved unforgeable against the super Type I adversary and super Type II adversaries. Hence, the security is robust, but the computational cost is high, computed in 2.82 MS for online user transactions. Similarly, the authors in [14] proposed a robust transaction scheme for mobile payments. This scheme is immune against four main types of attacks: MITM, impersonation, replay, and DoS. The scheme is designed based on strong certificate-less signatures with bilinear pairing crypto primitives integrated into the proposed transaction scheme. The security of this proposed mobile payment scheme depends on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (E.C.D.L.P.) and the intractability of breaking a bilinear pairing. Then, the authors evaluated the security robustness and practicability of their scheme. They prove that the security scheme guarantees robustness effectively against four attacks by implementing a transaction repository based on a private Blockchain network with smart contract technology. However, the smart contract used is often time-consuming to understand the risks associated with results from different sources, even for security experts. The authors in [15] proposed to use different security approaches together to increase the security level of data transmission during communication between sender and receiver. They used cryptography and Steganography. Cryptography is used to change the form of data transmission by using cryptography algorithms such as R.S.A., D.E.S., A.E.S., ElGamal, etc. Steganography keeps data hidden from attackers and ensures transmission data safety by embedding data with images, audio, video files, etc. Also, the authors propose to use multiple cryptography algorithms one after another: D.E.S., A.E.S., and Blowfish. Finally, they gave the idea of how to implement the three algorithms of cryptography and Steganography. Also, it mentioned the reasons for choosing the three cryptography algorithms. For example, they selected A.E.S. because it is a highly defendable cryptographic algorithm, and Blowfish. After all, it is the strongest and fastest cryptographic algorithm in data processing and storage. However, they did not evaluate their proposed technique's security and performance, which may cost computational processes and time when applying three cryptography algorithms one after another and then using the result file to apply in Steganography. The author in [16] mentioned that traditional security systems did not meet the security requirements of recent wireless communication networks. So, the author introduced a technology of network security encryption for the transmission of warship data used in military fields. This technology is used for warship data transmitted through satellite communication and applied on a network layer in the Open Systems Interconnection (O.S.I.) Model. The secure communication protocol is designed to ensure bidirectional authentication between client and server and preserve the confidentiality of data transmission. The author obtained an encryption wheel key through chaotic map transformation to update the key values of 80 bits. The performance of chaotic mapping is proportional to the number of iterations, affecting the encryption and data transmission speeds, so the author considered this. The encryption algorithm uses symmetric and asymmetric encryption to authenticate parties and secure ship data. Unlike other researches, asymmetric encryption is applied without needing a third party. Finally, the author used a small experiment three times, applying different technologies: encryption, authentication, and communication, with average time and cost every time. However, some security areas still need to be tested, such as the integrity of the data transmitted. In [17], the authors proposed multilevel security for bank systems to secure online transactions from attacks. The multilevel security is based on Blowfish encryption for any transaction between clients at the same bank (intra-banking) and the A.E.S. algorithm for any transaction between clients from the bank and clients from another bank. These two encryption algorithms incorporated dual one-time passwords (OTP). All bank customers should have two mobile numbers registered for the OTP system. The first is the primary number to receive the first OTP, and the other is the confident number to receive the second OTP. The bank validates the dual OTP to accept any transaction. The analysis of this system shows that the security of the system is better and faster than others currently in use, such as R.S.A. However, using Blowfish and A.E.S. algorithms have issues regarding crucial sharing, and the system is still vulnerable to some attacks, such as inside-bank attacks. Also, having two mobile numbers is impossible for each customer.

The contemporary review shows that although numerous security methods have been designed to shield electronic-payment transactions, none is universally applicable. Every approach is associated with some advantages, such as added confidentiality, resistance to certain attacks, or convenience, but with some limitations, such as high computational expense, complexity, or unfeasibility in practical application. The results highlight the need to embrace multi-layering as well as context-dependent security models. The next table consolidates comparisons between some security methods discussed in this chapter.

Table 2: Comparison between previous research on secure electronic payment transactions

| Ref. | Security Technique | Security achievement | Tools | Strength | Weaknesses |
|---|---|---|---|---|---|
| [8] | Triple DES | Stronger than DES and other techniques billions of times | Rely on DES block diagram with 3 secret keys. | Achieve high level of security. | Slow processing and have issues in key sharing |
| [13] | Crypto modules depend on Certificateless Signature (CLS). | Secure against super Type I and Type II adversaries | Random oracle model and raspberry Pi series platform. | Easily implemented and tested. | Computational cost is high which is computed in 2.82 MS. |
| [14] | Strong certificateless signatures with bilinear pairing crypto primitives. | Robustness effectively against four attacks: MITM, impersonate, replay, and DoS. | Raspberry Pi and implement a transaction repository with the aid of smart contract technology. | Easily implemented with acceptable computational cost. | Complexity in implementing and understanding smart contracts and the scheme needs other security features |
| [15] | Cryptography (DES, AES, and Blowfish) and Steganography. | Data Confidentiality. | LSB, DWT and DCT techniques for steganography. | High security by applying different security approaches. | High-cost Computational Process and Time. |
| [16] | Symmetric and asymmetric encryption | Confidentiality and bidirectional authentication. | Chaotic map transformation. | Lightweight encryption algorithm. | Limited testing of data integrity and Encryption performance is dependent on iteration count |
| [17] | Blowfish and AES incorporated with OTP system. | The security of the system is better and faster than others that are currently in use. | Core i3, 7th generation machine with JDK implementation and a database backend. | Faster and more secure compared to RSA Improved confidentiality for intra- and interbank transactions | Requires two mobile numbers for OTPs Vulnerable to inside-bank attacks |
| [18] | Certificateless cryptography for mobile payments. | Strong protection against adversaries and secure mobile transactions. | Android Pay integration with CLS modules. | Eliminates need for certification authorities; robust against attacks. | High computational resource demand. |
| [19] | Blockchain integrated with smart contracts. | Enhances transaction integrity and transparency. | Private blockchain networks. | Resistant to replay and impersonation attacks. | Time-consuming to implement; scalability challenges. |

## 3. The Security of Electronic Payment Protocols

An electronic payment protocol is an ordered list of steps applied to perform an electronic payment. The electronic transaction is a process that must be included in any electronic payment protocol. Several electronic payment protocols are discussed below and compared.

A secure protocol was proposed in [20] to handle accountability issues during payment transactions and ensure trust between mobile payment parties. The authors mentioned that their proposed protocol fulfills all security features required to build trust between parties in any payment system: confidentiality, authorization, mutual authentication, integrity, and non-repudiation. The accountability protocol proposed is based on symmetric and asymmetric encryption processes, so it needs initially to generate session keys for all three parties: buyer, seller, and payment gateway, such as a bank. Then the proposed payment protocol started in six steps, shown in Figure 3.

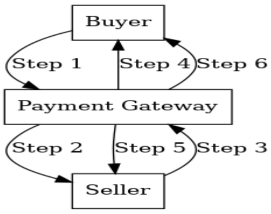

Figure 3: Message flows of the proposed protocol.

In the first step, the buyer sends a message hashed and encrypted with his private key to the gateway. This message authenticates the buyer to the gateway and ensures the integrity of the order information. In the second step, the gateway sends two messages to the seller. One is used to authenticate buyers, and another to mutually authenticate the gateway and seller. In the third step, the seller computes a hashed and encrypted message with the session key and then with the seller's private key and sends it to the gateway. This message ensures the integrity of the message and verifies that the seller is the receiver. In the fourth step, the gateway sends the remainder of the buyer's credit account hashed and encrypted message by session key to ensure the buyer can decrypt it, and by the private gateway key to authenticate that the gateway is the creator. In the fifth step, the gateway sends a message to the seller to notify that the buyer has now paid for his goods or services. In the last step, the gateway sends a message to the buyer to inform him that the price has been dropped from his account. Finally, the authors proved their proposed protocol's correctness and ensured its strength by analyzing the security using special tools. However, the proposed protocol is still vulnerable to attacks, such as impersonated attackers who steal the buyer's identity and establish sessions with the gateway and seller because there are no mechanisms to ensure the buyer's identity. Also, the mechanism of creating and distributing each party's public and private keys needs to be mentioned; it may be vulnerable.

Another protocol, which is an improvement on Secure Electronic Transaction (SET), was proposed to overcome some of the deficiencies in traditional encryption and decryption algorithms. With the incorporation of Elliptic Curve Cryptography (ECC) and Non-Adjacent Form (NAF) scalar multiplication, this protocol offers increased security and computational efficiency with reduced resource consumption. The system incorporates double digital signatures for added integrity and confidentiality during e-commerce transactions. Verification of this protocol through tools like Prover if ensures its strength. However, frequent authentications for a user changing devices and key management remain some of the challenging issues [21].

The authors in [22] proposed a new scheme for network communication that connects customers directly to their banks through mobile phones. The scheme aims to achieve the needs of all stakeholders and perform a high level of security without affecting efficiency and having a trusted infrastructure. The scheme will save time in implementation and marketing by reducing the overhead on all stakeholders. For each transaction, the issuer bank requests the verification code from the sender (buyer) that was sent before by the speedy pay system. The verification code helps ensure each transaction's integrity to prevent unauthorized transactions. The program's security, however, depends on affiliated banks' security, which must be guaranteed appropriately. Evidence in this system cannot be guaranteed in the event of security breaches. This plan must also guarantee communication and application security.

The centralized mobile payment protocol had to overcome a number of privacy issues; therefore, a design using partially blind signatures together with zero-knowledge proofs was introduced. It gives assurance that the TPSP will not trace an individual transaction, though regulatory compliance may still be tracked. The usage of security tags in this scheme provides fraudulent double-spending detection without affecting the anonymity of the user. Lightweight authentication mechanisms can also be embedded in the scheme to enhance transaction efficiency with unauthorized access prevention [23].

The authors suggested a mobile payment mechanism using near-field communication (N.F.C.) in [4]. The suggested protocol requires complete information security and equitable exchange characteristics in all sales transaction operations. The protocol used offline session key generation, symmetric and asymmetric encryption, and hashing. The protocol uses the offline session key generation method to increase security while preserving lightweight characteristics. It no longer needs to share the session key online using the offline session key-generating method. First, the protocol and the parties create the requirements. After that, each connection's session value is calculated by hashing the initial value. For all transactional data to remain encrypted and prevent decryption, a trusted third party must be included in the protocol. This encrypted data will be used as proof if a disagreement occurs. Burrows, Abadi, and Needham (B.A.N. logic) were used to verify the protocol by employing B.A.N. logic and the Scyther tool. To keep three values with others and generate a hash function, each entity in this protocol must perform computational work at each step. The program's security, however, depends on affiliated banks' security, which must be guaranteed appropriately. Evidence in this system cannot be guaranteed in the event of security breaches. This plan must also guarantee communication and application security. This protocol is vulnerable to attacks involving insiders, stolen smart Cards, physically stolen equipment, and unauthorized critical computations.

Similarly, the author [24] suggested an authentication procedure for N.F.C. connection in the context of mobile payments. The authentication problems and fairness were proposed as solutions by this protocol. The proposed protocol employs the offline session key generation technique to increase the transaction's security and maintain lightweight while having fairness properties. The protocol used secure session key distribution based on symmetric key encryption. The protocol was conducted in four phases: initiation phase, registration phase, authentication phase, and dispute resolution phase. The protocol satisfies the essential properties of information security and vital fairness necessary in each mobile payment system regarding building trust between all parties associated with the transaction. The protocol was verified using B.A.N. logic, the Scyther tool, and A.V.I.S.P.A. to verify the security protocol. However, this protocol fails to ensure communication and application security. The protocol cannot resist insider, stolen smartcard, physically stolen devices, and unauthorized critical computation attacks. Also, [4]. and [24] have disadvantages in employing the offline session key generation. If the initial value of the shared triple is exposed, then the attacker can generate all the session keys of later stages. The generation method of offline session keys has been developed in [25] to prevent sharing the session key through the network.

Classic NFC protocol improvements have also taken into consideration security by implementing secure mutual authentication. Based on the usage of shorter key lengths in ECC, and high resistance against brute force attack attempts, key exchange mechanisms that are dynamic are now incorporated. Privacy-preserving attributes, such as partial blind signatures, for example, will ensure that even during an active transaction, sensitive information about the user remains hidden. This provides better compliance with emerging privacy laws and reduces the risks of unauthorized tracking or data breaches [23], [21].

Another innovative feature of the enhanced SET protocol is to adopt a multi-layered security approach that includes strong encryption at the hardware level, communication security, and application-level security. Using ECC-based digital signatures, SET ensures that transactions are tamper-proof and resistant to replay attacks. The modular architecture of this protocol makes it easily embeddable in different e-commerce platforms and thus adaptable and scalable [23]. In mobile payments, the mutual zero-knowledge authentication between merchants and customers was introduced. Since it enables one to prove his or her identity without revealing any sensitive information, this approach is not only privacy-preserving but also provides resistance against impersonation and man-in-the-middle attacks. These improvements target long-standing gaps in trust and data integrity in centralized payment systems [21].

The authors in [26] have proposed a new protocol for N.F.C. mobile payment. The protocol enhances mutual authentication by using an asymmetric encryption method, which improves the global system for mobile (GSM) authentication protocol due to security threats of symmetric cryptography and uses public key encryption. In addition, it decreases the number of critical pairs required for authentication from four to three key pairs. The protocol decreases the processing and signalling overhead on the client side as much as possible because mobile devices have limited processing power and resources. This protocol aims to enhance mobile payment security based on N.F.C. protocol focusing on securing authentication and preventing attacks such as replay, denial of service (D.O.S.), eavesdropping attacks, repudiation, a man-in-the-middle attack, and de-synchronization. The protocol is conducted in three phases: authentication, authorization, and transaction. Evidence cannot be guaranteed under this protocol in the event of a security breach. Moreover, this protocol does not guarantee end-to-end security and is susceptible to multi-protocol assaults and reverse engineering.

The author proposed a secure mobile payment mechanism based on Near Field Communication [27]. (N.F.C.). The concept suggested three levels of defence in depth: defence at the level of mobile applications, communication, and hardware. The suggested protocol offers protection from multiple attacks, including denial of service, distributed denial of service, and assaults using random access memory scraping and multiple protocols. The suggested approach ensures security characteristics and circumvents known mobile application vulnerabilities like Heartbleed. The proposed protocol was successfully verified using the Scyther tool and B.A.N. logic. Evidence cannot be guaranteed under this protocol in case of security breaches.

The study of existing electronic payment protocols reflects notable developments in securing online and mobile transactions by means of encryption, authentication, and formal verification techniques. Though most proposed protocols have high levels of confidentiality, non-repudiation, and mutual authentication, they are lacking in evidence generation, robustness to insider attacks, and practical scalability. In particular, certificateless mechanisms using NFC-based protocols have potential but need further development to combat ongoing vulnerabilities. The following table is a comparative overview of such protocols.

Table 3: Comparison between previous research on securing electronic payment protocols

| Ref. | Protocol used | Security Technique | Formal Verification | Evidence guarantees | Security achievement | Weaknesses |
|---|---|---|---|---|---|---|
| [20] | Mobile payment. | Symmetric and asymmetric encryption. | Yes | Yes | Confidentiality, authorization, mutual authentication, integrity, and non-repudiation. | Still vulnerable for some attacks such as: impersonated attacker. |
| [21] | Privacy-preserving centralized payment | Zero-knowledge proofs and partially blind signatures | Yes | Yes | Ensures anonymity, prevents double-spending, and strengthens user privacy | Complexity in implementation and reliance on TPSP for token issuance |
| [22] | Instant mobile payment. | Using speedy pay system. | False | False | Perform a high level of security, saving time, reducing the overhead on all stakeholders, and ensuring the integrity of each transaction to prevent any unauthorized transactions. | Evidence cannot be guaranteed and does not ensure communication and application security. |
| [23] | SET with ECC and NAF | ECC with improved NAF scalar multiplication | Yes | False | Enhances security and computational efficiency; provides tamper-proof transactions | Challenges in user device compatibility and key management |
| [4] | NFC mobile payment. | Used both symmetric and asymmetric encryption, hash function, and offline session key generation | Yes | Yes | Possesses comprehensive features of information security while maintaining lightweight features. | Have disadvantages of employing the offline session key generation and still vulnerable some attacks. |
| [24] | NFC mobile payment. | Based on symmetric key encryption and employs the offline session key generation technique. | Yes | Yes | Overcome the authentication issues and satisfies the essential properties of information security. | Have disadvantages of employing the offline session key generation and still vulnerable some attacks. |
| [26] | NFC mobile payment. | Using asymmetric encryption method to improve GSM authentication. | Yes | False | Securing authentication and preventing attacks such as: replay, denial of service (DOS), eavesdropping attacks, repudiation, man in the middle attack and desynchronization. | Cannot guarantees evidence and still vulnerable some attacks. |
| [27] | NFC mobile payment. | AES and Elliptic Curve Digital Signature Algorithm (ECDSA) | Yes | False | Has all the security properties, overcomes most of attacks, and defense in depth of 3 levels. | Evidence cannot be guaranteed in case of security breaches. |

## 4. Integrated Analysis and Evaluation the Security of Electronic Payments

With digital payment systems becoming the backbone of contemporary commerce, the requirement for resilient and dynamic security measures has never been more critical. Electronic payment systems need to be not only fast and easy but also secure against an expanding array of threats in cyberspace. This section offers a combined study of the leading security measures and techniques in electronic payments and their effectiveness, shortcomings, and practicality.

One of the more widely debated innovations includes certificateless cryptographic protocols. Such schemes eliminate the need to rely on conventional Public Key Infrastructure (PKI) by not having certificate authorities, reducing key management and communication overhead. Certificateless signatures have proved to be very proficient at avoiding impersonation, eavesdropping, and man-in-the-middle attacks [19]. One of their key shortcomings, however, is computational intensity, particularly a drawback in mobile and resource-limited contexts where there is limited processing power and battery life.

Blockchain technology is also a revolutionary solution in this field, especially in the case of transaction integrity and auditing. Through distributed ledgers and smart contracts. The complexity associated with the implementation of smart contracts and latency in transaction validation are still challenges that pose considerable issues, especially in real-time payment applications and supporting large volumes of them.

More advanced hybrid cryptographic methods by integrating classical encryption schemes (AES, RSA) with steganography add yet another level of protection by hiding encrypted data within multimedia. This two-layered process increases both secrecy and interference resistance. However, the sequential execution of algorithms increases computational cost considerably, and such methods are not feasible over real-time scenarios or mobile devices without optimization.

In the meantime, more lightweight cryptographic technologies like elliptic curve cryptography (ECC) and chaotic map transformations are finding favour due to their efficiency and appropriateness in power-constrained settings such as IoT-based payment systems. Such technologies can make a trade-off between security and performance, especially in cases where there are limited resources to process [23]. Whereas they are excellent at ensuring confidentiality and authentication, more research should be done to ensure their effectiveness in maintaining integrity and system availability under various threats.

In comparison to this, NFC-based payment protocols have better mutual authentication and faster data exchange to enable faster transactions. However, they are susceptible to both relay and proximity-based attacks and do not have end-to-end encryption.

By and large, the comparative analysis shows that no single protocol can meet all security and performance needs. Certificateless protocols are secure but computationally expensive, blockchain guarantees trust but is not very scalable; models that offer strong confidentiality require computational effort, and efficient lightweight schemes compromise efficiency for limited assurance. Therefore, the optimal approach is an overlayered security architecture that utilizes multiple mutually supportive techniques that have been optimized based on use cases and device capabilities.

There is no single security mechanism that addresses all e-payment issues. The key is multi-layered, adaptive systems leveraging strengths of each technique, optimized to use case, platform, and user environment. Such systems must ensure security along with ease of deployment, interoperability, and scalability for wide adoption and long-term viability. Future research should optimize lightweight algorithms to reduce client-side costs, and develop context-specific, modular solutions to ensure robust protection and operational feasibility across diverse environments.

## 5. Research Gaps and Future Directions

Although many studies have improved confidentiality, authentication, and integrity in electronic payment systems, several underexplored areas remain. First, tokenization and blockchain integration for secure, scalable, and privacy-preserving transactions are still in the early stages. Few works address lightweight security mechanisms optimized for mobile and IoT devices, where computational resources are limited. Additionally, existing protocols rarely align security mechanisms with regulatory compliance (e.g., PCI-DSS, PSD2) in a dynamic and adaptive way. Finally, human-centric factors such as usability, user trust, and real-time fraud analytics have received limited academic attention. Addressing these gaps can lead to more robust and deployable secure payment frameworks.

In conclusion, making future electronic payments secure will involve a collaborative effort that merges cryptography, machine learning, system design, and user behaviour. This convergence holds the possibility for an integrated, adaptive, and user-focused security system for next-generation payment systems.

## 6. Conclusion and Future Work

Secure electronic payments are a necessity in the era of online and mobile transactions. This article discussed new developments and vulnerabilities in e-payment systems, emphasizing encryption, authentication, blockchain, and certificateless cryptography. Although no system is fully secure, reliable systems minimize breaches by ensuring confidentiality, authentication, authorization, integrity, and non-repudiation while resisting threats such as impersonation, eavesdropping, and denial-of-service. They should also generate verifiable evidence to support forensic analysis. With the increasing use of mobile and IoT devices, future models must use lightweight security mechanisms that minimize client overheads, while hybrid cryptographic solutions with optimized smart contracts offer promise. Security should be based on enhanced multi-layered architectures that combine conventional cryptography with innovative methods, balancing protection with performance to strengthen trust and global adoption.

## References

[1] S. F. Verkijika, An effective response model for understanding the acceptance of mobile payment systems, Electronic Commerce Research and Applications 39 (2020) 100905, https://doi.org/10.1016/j.elerap.2019.100905.

[2] M. Baza, N. Lasla, M. M. Mahmoud, G. Srivastava, M. Abdallah, B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain, IEEE

Transactions on Network Science and Engineering 8 (2) (2019) 1214–1229, https://doi.org/10.1109/TNSE.2019.2959230.

[3] R. M. Mohammad, H. Y. AbuMansour, An intelligent model for trustworthiness evaluation in semantic web applications, In 2017 8th international conference on information and communication systems (ICICS), IEEE (2017) 362–367, https://doi.org/10.1109/IACS.2017.7921999.

[4] C. Thammarat, W. Kurutach, A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification, International Journal of Communication Systems 32 (12) (2019) e3991, https://doi.org/10.1002/dac.3991.

[5] R. L. Rivest, A. Shamir, PayWord and MicroMint: Two simple micropayment schemes, in International workshop on security protocols, Springer (1996) 69–87, https://doi.org/10.1007/3-540-62494-5_6.

[6] M. Farion, A. Farion, Security of Mobile Payments and Digital Wallets, https://dspace.wunu.edu.ua/bitstream/316497/37537/1/SECURITY%20OF%20MOBILE%20PAYMENTS%20AND%20DIGITAL%20WALLETS%2019.docx, [accessed 11.11.2025].

[7] W. Ahmed, A. Rasool, A. Javed, N. Kumar, T. Gadekallu, Z. Jalil, Security in next generation mobile payment systems: A comprehensive survey, IEEE Access 9 (2021) 115932–115950, https://doi.org/10.1109/ACCESS.2021.3105450.

[8] S. Mitra, B. Jana, J. Poray, Implementation of a novel security technique using triple des in cashless transaction, In 2017 international conference on computer, electrical & communication engineering (ICCECE), IEEE (2017) 1–6, https://doi.org/10.1109/ICCECE.2017.8526233.

[9] B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, A. A. Langoo, S. Assad, A compendious study of online payment systems: Past developments, present impact, and future considerations, International journal of advanced computer science and applications 8 (5) (2017) 256-271, http://dx.doi.org/10.14569/IJACSA.2017.080532.

[10] K. AL-Qawasmi, M. AL-Mousa, M. Yousef, Proposed e-payment process model to enhance quality of service through maintaining the trust of availability, arXiv preprint arXiv:2101.01399 (2021), https://doi.org/10.48550/arXiv.2101.01399.

[11] Z. Hasan, C. Agrawal, M. Agrawal, online transaction security enhancement: An algorithm based on cryptography, In 2019 international conference on issues and challenges in intelligent computing techniques (ICICT), IEEE (2019) 1–4, https://doi.org/10.1109/ICICT46931.2019.8977669.

[12] H. Kader, M. Hadhoud, Performance evaluation of symmetric encryption algorithms, International Journal of Computer Science and Network Security 8 (12) (2008) 280–286.

[13] K.-H. Yeh, A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments, IEEE Systems Journal 12 (2) (2017) 2027–2038, https://doi.org/10.1109/JSYST.2017.2668389.

[14] K.-H. Yeh, C. Su, J.-L. Hou, W. Chiu, C.-M. Chen, A robust mobile payment scheme with smart contract-based transaction repository, IEEE Access 6 (2018) 59394–59404, https://doi.org/10.1109/ACCESS.2018.2874021.

[15] P. K. Singh, P. Tripathi, R. Kumar, D. Kumar, Secure data transmission, International Research Journal of Engineering and Technology 4 (4) (2017) 217–222.

[16] L. Xu, Secure transmission strategy of network communication layer relay based on satellite transmission, In 2020 2nd international conference on information technology and computer application (ITCA), IEEE (2020) 268–271, https://doi.org/10.1109/ITCA52113.2020.00064.

[17] G. Muneeswari, A. Puthussery, Multilevel security and dual OTP system for online transaction against attacks, In 2019 third international conference on i-SMAC (IoT in social, mobile, analytics and cloud) (i-SMAC), IEEE (2019) 221–225, https://doi.org/10.1109/I-SMAC47947.2019.9032466.

[18] S. E. Cebeci, K. Nari, E. Ozdemir, Secure e-commerce scheme, IEEE Access 10 (2022) 10359–10370, https://doi.org/10.1109/ACCESS.2022.3145030.

[19] Y. Liu, W. Huang, M. Zhuo, S. Zhou, M. Li, Mobile payment protocol with deniably authenticated property, Sensors 23 (8) (2023) 3927, https://doi.org/10.3390/s23083927.

[20] C. Thammarat, C. Techapanupreeda, A secure mobile payment protocol for handling accountability with formal verification, In 2021 international conference on information networking (ICOIN), IEEE (2021) 249–254, https://doi.org/10.1109/ICOIN50884.2021.9333957.

[21] C.-M. Yu, X. Jin, A. Feng, Secure e-commerce payment system based on novel SET network protocols, Journal of Network Intelligence 9 (2) (2024) 881-895.

[22] M. Obaid, Z. Bayram, M. Saleh, Instant secure mobile payment scheme, IEEE Access 7 (2019) 55669–55678, https://doi.org/10.1109/ACCESS.2019.2913430.

[23] J. Neera, X. Chen, N. Aslam, B. Issac, A trustworthy and untraceable centralised payment protocol for mobile payment, ACM Transactions on Privacy and Security, 28 (2) (2025) 1-29, https://doi.org/10.1145/3706421.

[24] C. Thammarat, Efficient, secure NFC authentication for mobile payment ensuring fair exchange protocol, Symmetry 12 (10) (2020) 1649, https://doi.org/10.3390/sym12101649.

[25] R. A. Abouhogail, A. H. Ali, Design and development of an advanced authentication protocol for mobile applications using NFC technology, Journal of Computer Science 15 (12) (2019) 1809–1819, https://doi.org/10.3844/jcssp.2019.1809.1819.

[26] F. S. M. Tafti, S. Mohammadi, M. Babagoli, A new NFC mobile payment protocol using improved GSM based authentication, Journal of Information Security and Applications 62 (2021) 102997, https://doi.org/10.1016/j.jisa.2021.102997.

[27] S. S. Ahamad, A novel NFC-based secure protocol for merchant transactions, IEEE Access 10 (2021) 1905–1920, https://doi.org/10.1109/ACCESS.2021.3139065.

[28] E. N. C. Granja, Developing a Next-Generation Tokenization Framework to Secure Digital Payments, https://www.authorea.com/users/824284/articles/1221046-developing-a-next-generation-tokenization-framework-to-secure-digital-payments, [accessed 11.11.2025].