Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526
Volume 14 Issue 01, 2025

Cryptography in Digital Payments: Ensuring Secure and Trustworthy Financial Transactions

Mayank S. Dudhe[1], Harsh A. Patil[2], Rahul Z. Thawkar[3], Kunal D. Mohrale[4,] Mr. Rahul Lilhare[5]

[1-5]MCA Department Suryodaya College of Engineering & Technology, Nagpur
mayankdudhe12@gmail.com[1],1234harshpatil@gmail.com[2],rahulthawkar2000@gmail.com3,kdmoharle@gmail.com[4], rklilhare661@gmai.com[5]

Peer Review Information

Submission: 11 Feb 2025
Revision: 20 Mar 2025
Acceptance: 22 April 2025

Keywords

RSA
Elliptic Curve Scheme
Digital Signature
Encryption And Decryption

Abstract

Since the mobile systems are growing quickly, the e-commerce will change gently to m-commerce. As a result, mobile security will become the one of the most important part of mobile system and will become the hottest area facing the mobile payment due to mobile networks directness. However, the appropriate encryption scheme for mobile communication must have small amount of data calculating and quick operation as of its inherent restrictions of small quantity and low calculating ability. The objectives of this paper are to look at mobile payment and its security. Also, to explain elliptic curve with public key encryption, authentication of security wireless milieu. Compare with the RSA scheme, an elliptic curve has shorter key size, smaller signature length, low calculating, fast operations and high security working.

Introduction

Digital payments have become an integral part of modern financial systems, offering consumers and businesses a fast, convenient, and efficient way to conduct transactions. From mobile wallets and online banking to e-commerce platforms and contactless payments, the adoption of digital payment solutions continues to grow globally. This shift towards cashless transactions is driven by technological advancements, increased internet accessibility, and the demand for seamless financial services.

However, with the rise in digital transactions, the risk of cyber threats and financial fraud has also increased. Malicious actors often target sensitive financial data, leading to data breaches, identity theft, and unauthorized access to funds. Ensuring the security and privacy of digital payments is paramount to maintaining user trust and safeguarding financial assets. Strong security measures are essential to protect transaction data, verify user identities, and prevent unauthorized activities.

Cryptography serves as a fundamental solution to address these security challenges. It involves the use of mathematical algorithms to encrypt and decrypt data, ensuring that sensitive information remains confidential and accessible only to authorized parties. Additionally, cryptography provides authentication mechanisms to verify the legitimacy of users and transactions, while also ensuring data integrity by preventing unauthorized alterations.

This research paper delves into the role of cryptography in securing digital payments. It examines various cryptographic techniques, including symmetric and asymmetric encryption, hash functions, and digital signatures. Furthermore, it explores the implementation of cryptographic protocols in payment systems,

highlighting their effectiveness in preventing cyber threats. By understanding the critical role cryptographplays in digital payment security, this study aims to provide valuable insights into strengthening the resilience of financial ecosystems in the digital age.

Fundamentals Of Cryptography

Cryptography is the science of securing information through mathematical techniques, ensuring confidentiality, integrity, and authenticity. It is widely used in digital payments to protect sensitive data, verify user identities, and prevent unauthorized access. Understanding the fundamental concepts of cryptography is essential to grasp its role in securing financial transactions.

Basic concepts of cryptography

Encryption: Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) using a cryptographic algorithm and a key. This ensures that the data remains confidential and can only be accessed by authorized parties.

Decryption: Decryption is the reverse of encryption. It involves converting the ciphertext back into plaintext using the appropriate key. Only the intended recipient with the correct key can decrypt the data.

Keys: Keys are essential in cryptography, serving as unique parameters for encryption and decryption. Keys are classified into two types: symmetric keys (same key for both encryption and decryption) and asymmetric keys (a pair of public and private keys).

Algorithms: Cryptographic algorithms are mathematical functions used to encrypt and decrypt data. Popular algorithms include Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC).

Symmetric Vs. Asymmetric Cryptography

Symmetric cryptography

1. In symmetric cryptography, the same key is used for both encryption and decryption.
2. It is efficient and faster, making it ideal for encrypting large amounts of data.
3. Common algorithms: AES, DES (Data Encryption Standard), and Blowfish.
4. **Example**: Secure Socket Layer (SSL) uses symmetric encryption for fast data transmission in digital payments.

Asymmetric cryptography

1. Asymmetric cryptography uses a pair of keys: a public key (for encryption) and a private key (for decryption).
2. It is commonly used in secure communications and digital signatures.
3. Algorithms like RSA and ECC are widely used in digital payment systems.
4. **Example**: Payment gateways use asymmetric encryption to secure sensitive payment information.

Hash Functions And Digital Signatures

Hash functions

1. A hash function is a one-way cryptographic algorithm that converts input data into a fixed-length hash value (digest).
2. Hashing ensures data integrity by detecting any changes made to the original data.
3. Common hash functions: SHA-256 (Secure Hash Algorithm) and MD5 (Message Digest Algorithm).
4. **Example**: Hashing is used to securely store passwords and verify transaction data in digital payment systems.

Digital signatures

1. Digital signatures provide authentication, data integrity, and non-repudiation in digital transactions.
2. They use asymmetric cryptography to sign and verify messages.
3. A private key is used to create a digital signature, and a public key is used for verification.
4. **Example**: Digital signatures are widely used in digital payment gateways and financial documents to ensure transaction authenticity.

Types Of Cryptographic Algorithms Used In Digital Payments

Cryptographic algorithms play a crucial role in securing digital payment systems by ensuring data confidentiality, integrity, and authentication. Various algorithms are used based on the requirements of payment platforms, including speed, security, and resource efficiency.

RSA (Rivest-Shamir-Adleman):
RSA is a widely used asymmetric encryption algorithm that uses a pair of public and private keys for secure data transmission. It is often applied in digital signatures and secure key exchanges in payment gateways to ensure transaction authenticity and confidentiality.

AES (Advanced Encryption Standard)
AES is a symmetric encryption algorithm known for its speed and security. It uses key sizes of 128,

192, or 256 bits, making it highly effective for encrypting large amounts of payment data. AES is commonly used in contactless payment systems and mobile wallets for secure data storage and transmission.

ECC (Elliptic Curve Cryptography)
ECC is an asymmetric encryption technique that offers robust security with shorter key sizes compared to RSA. This makes it ideal for resource-constrained devices like smartphones and payment terminals. ECC is widely used in mobile payment applications and digital wallets due to its efficiency and strong encryption capabilities.

SHA (Secure Hash Algorithm):
SHA is a cryptographic hash function that generates a fixed-length hash value from input data. It ensures data integrity by detecting unauthorized changes to payment information. SHA-256, a variant of SHA, is extensively used in digital signatures, blockchain-based payment systems, and secure transaction verification.

Mobile payment system
Secure milieu for mobile payment scheme is shown in figure 1. It includes seven components: customer, merchant, mobile network operator (MNO), bank, trusted authority (TA), information center (IC) and certificate authority (CA). Time stamping server (TSS) gives notarization from the neutral viewpoint if challenge happens. The system is relied on the SEMOPS (Secure Mobile Payment Service), but enhancements to the SEMOPS are made to deal with the signature validation and confidentiality issues. In the system, MNO can be work as the user payment processor in addition to the role of wireless access provider. In general, the bank is the customer accounts holder. So the bank is more appropriate as the payment processor. TA is the part, where CA and TSS, to give notarization from the neutral viewpoint if challenge happens. IC is similar as in SEMOPS; it is in charge for routing and distributing notifications to recipient payment processor.

Cryptography in mobile and online payments
Cryptography is a cornerstone of security in mobile and online payment systems, ensuring that financial transactions remain secure from unauthorized access and cyber threats. Various cryptographic techniques and technologies are implemented to protect sensitive data during payment processes.

End-to-end encryption (e2ee)
E2EE ensures that data is encrypted on the sender's device and can only be decrypted by the intended recipient. In mobile and online payments, this prevents intermediaries, such as service providers or hackers, from accessing sensitive information like card details and personal data. Payment apps and digital wallets often use E2EE to maintain transaction confidentiality.

Biometric authentication and multi-factor authentication (mfa):
Cryptographic systems often integrate biometric authentication (such as fingerprint scans, facial recognition, or iris scans) to verify a user's identity. Multi-factor Authentication (MFA) adds an additional layer of security by requiring users to authenticate using two or more factors, including passwords, biometrics, or one-time passcodes. These methods ensure secure access to payment platforms and prevent fraudulent transactions.

Blockchain and cryptocurrencies in payment systems
Blockchain technology leverages cryptographic hashing and digital signatures to maintain a decentralized and tamper-resistant ledger of transactions. Cryptocurrencies like Bitcoin and Ethereum use blockchain to secure peer-to-peer payments without the need for intermediaries. Smart contracts, powered by blockchain, further enhance security by automatically executing payment agreements based on predefined conditions.

Conclusion
In the rapidly evolving digital payment landscape, cryptography plays a pivotal role in ensuring the security, privacy, and integrity of financial transactions. Through the use of advanced cryptographic algorithms like RSA, AES, ECC, and SHA, digital payment systems protect sensitive information from cyber threats and unauthorized access. Real-world implementations in platforms like Apple Pay, Google Pay, and PayPal demonstrate the effectiveness of encryption, tokenization, and secure authentication mechanisms. Additionally, technologies like blockchain and digital signatures further enhance transparency and trust in decentralized payment systems.
However, emerging challenges such as the advent of quantum computing pose significant threats to existing cryptographic standards. To mitigate these risks, the development and adoption of post-quantum cryptography (PQC) are essential. Furthermore, leveraging AI-powered cryptographic systems can enhance threat detection, optimize encryption processes, and ensure real-time protection against sophisticated cyberattacks.

To strengthen digital payment security, financial institutions and payment service providers should implement comprehensive security measures, including end-to-end encryption (E2EE), multi-factor authentication (MFA**)**, and robust key management systems. Additionally, fostering collaboration between regulators, technology developers, and cybersecurity experts is crucial to establish consistent security standards and regulatory compliance across regions.

Continued investment in research and innovation, along with regular security audits and incident response protocols, will further fortify digital payment systems against emerging threats. By adopting proactive cryptographic measures and staying ahead of evolving cyber risks, stakeholders can ensure a secure, resilient, and trustworthy digital financial ecosystem.

References

W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Upper Saddle River, NJ, USA: Pearson, 2017.

B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. Hoboken, NJ, USA: John Wiley & Sons, 1996.

R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology (CRYPTO '82)*, 1982, pp. 199-203.

S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Advances in Cryptology – EUROCRYPT '94*, 1994, pp. 92-111.

V. Shoup, *A Computational Introduction to Number Theory and Algebra*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2009.

A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, Jan. 1987.

D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology – CRYPTO '01*, 2001, pp. 213-229.

A. Bhargavan, K. Bhargavan, and U. Ramanan, "Formal verification of smart contracts in digital payment systems," in *Proc. IEEE S&P Conf.*, 2020, pp. 1203-1217.

C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st ACM Symposium on Theory of Computing (STOC '09)*, 2009, pp. 169-178.