International Journal of Multidisciplinary Research and Growth Evaluation.

Implementing Payment System Security: A Technical Deep Dive

Balaji Soundararajan
Independent Researcher, USA

* Corresponding Author: **Balaji Soundararajan**

Article Info

ISSN (online): 2582-7138
Volume: 03
Issue: 05
September-October 2022
Received: 22-08-2022
Accepted: 19-09-2022
Page No: 615-621

Abstract
The rapid transition from cash-based to digital payment systems underscores the critical need for robust security frameworks to safeguard sensitive financial data and maintain public trust. This paper explores the foundational principles of payment system security that includes data integrity, confidentiality, and availability and examines key technologies and methodologies designed to mitigate risks, including encryption, tokenization, and authentication mechanisms. Symmetric and asymmetric encryption techniques are analyzed for their roles in securing transactional data, while tokenization is highlighted as a method to reduce exposure of sensitive information. Secure communication protocols such as TLS and multi-factor authentication (MFA), including biometric verification, are discussed as essential layers of defense against evolving cyber threats. The challenges of securing mobile payment systems and compliance with regulations like PCI DSS are also addressed. The study concludes that a multi-layered security approach, coupled with adherence to evolving standards and user education, is vital to sustaining trust in digital payment ecosystems.

DOI: https://doi.org/10.54660/.IJMRGE.2022.3.5.615-621

Keywords: Payment system security, symmetric encryption, asymmetric encryption, tokenization, multi-factor authentication (MFA), biometric authentication, secure communication protocols, PCI DSS, data integrity, mobile payment security

Introduction

Society is undergoing an unprecedented shift away from traditional cash-based economies and toward digital payments. Payment system security is crucial to sustaining the public's trust and preventing the theft or misuse of sensitive financial data. As more consumers rely on digital payments, the failure to secure their money erodes the public's faith and limits widespread adoption of nascent payment technologies. Malicious actors are quick to capitalize on this vulnerability. Reports indicate that cybercrime loss value in the US alone reached significant amounts, and estimates suggest that losses top substantial figures globally. Critical economic pillars like the financial sector become prime targets for cyberattacks. Payment systems, whose purpose is to communicate financial transactions from entities such as issuing banks to acquiring banks, are no exception. Secure communication of financial data is vitally important for a payment system to remain viable. Over the past decades, several stringent regulations have been enacted in the interests of secure communications in the payment ecosystem. Examples include various data security standards and regulations, which impose legal penalties on corporations found non-compliant.

New challenges arise for payment systems as technology advances and more businesses provide their services digitally. A major computer chip equipment provider forecasts non-contact payments using biometric data to be the future of payment transactions. In addition, the council responsible for payment card security laid out technologies that will shape payment security over the next couple of years. These include compatibility with popular e-commerce plugins, mobile application support, in-person payment system support, and various merchant and customer interfaces. Some of the system components affected by these interface changes are databases for merchant and entity data management, financial engine core workflows, authentication mechanisms such as biometrics, and sending and receiving transacted data.

Fundamentals of payment systems security

In a transactional context, security comes down to three fundamental principles:

- **Data Integrity:** Ensuring that transactional information being sent is the same information the recipient receives.
- **Confidentiality:** Preventing the transactional information from being read or otherwise acted upon by unintended parties.
- **Availability:** Keeping the entire transactional process – from a merchant approving a payment to a funds transfer – accessible at all times to authorized parties.

Centralized payment system information traveling over networks can be interrupted, altered, or even intercepted. The most common and familiar of these systems to consumers is the use of credit, debit, or charge cards – but there are a number of others including digital wallets and cryptocurrencies. These payment systems occur in person and remotely and rely on information security experts to maintain a safe and secure end-to-end process. Most of the trusted endpoint information security devices and services transactional stakeholders rely on are poorly understood and can be hijacked or bypassed for malicious means. Failure to detect and potentially bypass these vital technological safety net areas could lead to fraud loss or data breach. Similar to notorious bypass fraud and other fraud scams, there are a number of data breach and hacker threats to the payment systems that appear in the news daily. One of the most difficult requirements for businesses and non-technology savvy individuals is the security standards for the payment card industry, and everyone involved with the payment ecosystem must adhere to these standards for payment system security from technological penetration. Technology and security protocols aside, the customer is just as important in containing the electronic cyber threat. It is equally important that the transaction chains within the payment ecosystem are practicing customer trust for system assurance for their payment transactions. Out of compliance with an approved scanner of remote computers or networks connected to the open internet is not such a great idea if you are involved as a business in the payment system, regulator, examiner, or end-user cardholder. In an online scenario, payment system security designates how merchants verify fraudsters executing or malware residing in the payment session.

Encryption and tokenization in payment systems

Encrypting cardholder and sensitive payment information is a pivotal contribution to securing a payment system. With encryption, clear text in the form of plain data is morphed into encoded formats that prevent unauthorized access without associated decryption keys. Two primary types of encryption exist: symmetric and asymmetric. Symmetric encryption utilizes a shared secret key for both encoding and decoding. The two communication parties will use a secure technique to first agree on a common key. The key will then be used for secure communication for further data exchange before it is changed or renegotiated based on the agreement.

The main advantage of symmetric encryption is that since only one key is required, the associated cryptographic algorithm runs faster and has less computational burden compared to asymmetric encryption. Despite this speed concern, symmetric encryption is applicable for transaction key establishment in secure channels at a point of sale or an automated teller machine.

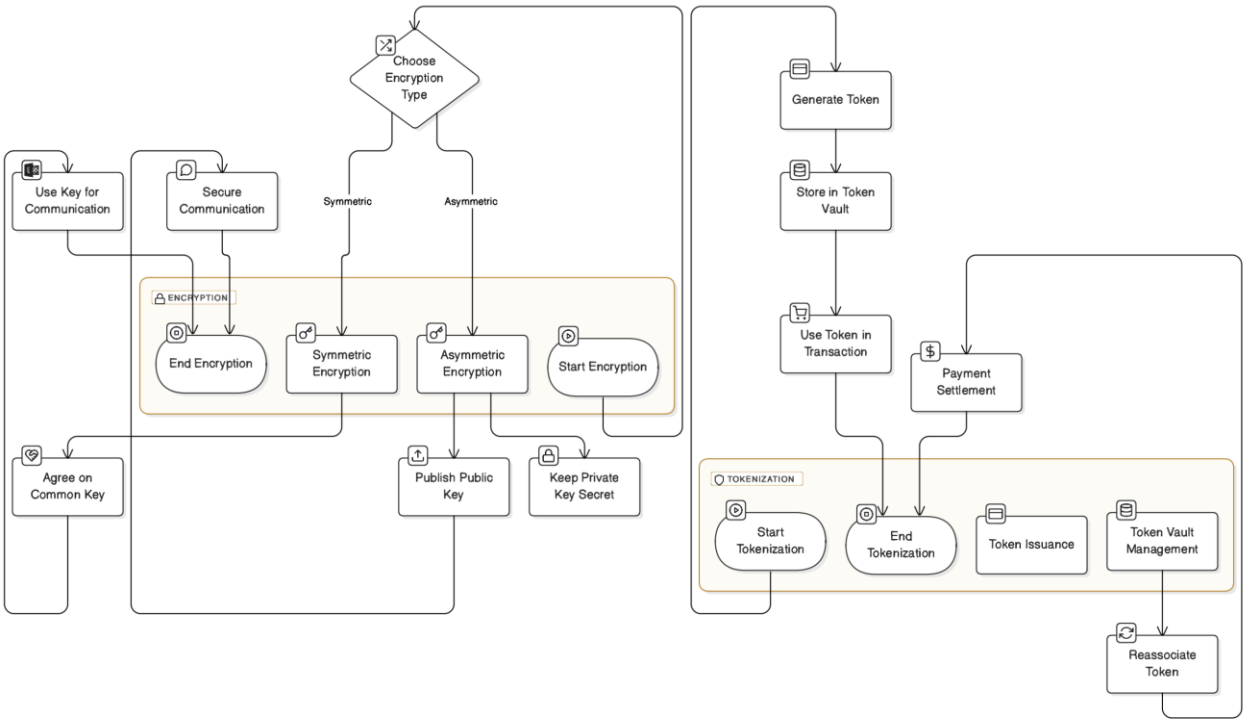

Fig 1

Asymmetric encryption, also known as public-private key encryption, is applied in situations that necessitate a secure communication channel between unknown or untrusted parties. As in symmetric encryption, a public key is published, while a private key is kept secret. There is no need to transmit the private key between the communicating parties, which also enforces strong confidentiality, non-repudiation, and integrity of the data. A potential use case is

in the security testing of EMV-based smart cards, where card authentication keys and verified cryptograms are validated on the payment network. In this particular application, it is impractical and sometimes technically challenging to have the credential operations processed in hardware secure elements within a payment terminal.

Tokenization is another strategy of securing sensitive payment data by replacing clear account numbers with a non-sensitive, or 'token,' that is effective only in a particular transaction context with the original merchant where the additional sensitive data is stored. In general, a token in payment processing is a surrogate for a primary account number. A token is issued by a token service provider or by a payment system operator that can be either the merchant, acquirer, or directly by a card network association. There are different techniques of tokenization, each offering a different level of security, cardholder data exposure, and acceptance. The fundamental concept behind all types involves a secure surrogate token vault where the original account number and the equivalent token are centrally stored and managed. Depending on the tokenization scheme, the card networks, banks, and other organizations related to the payment processing network will receive one or more of the original account number, its token, or both on a payment message. Payment schemes will mandate certain tokenization-for-secure-payment schemes as a privacy imperative and to comply with various regional and national data protection laws and regulations. Such tokenization solutions are maintained centrally in highly secured interoperable vaults for token creation and privacy preserving reassociation, a process of reverting the surrogate token to the original account number for payment settlement [1].

Symmetric and asymmetric encryption

In essence, encryption relies on two cryptographic concepts: simply put, there are two kinds of encryption methods: symmetric encryption and asymmetric encryption. One of the most significant differences between symmetric and asymmetric encryption lies in the number of keys they use. Symmetric encryption is much faster but uses the same key for both encryption and decoding, while an asymmetric encryption method uses a pair of keys, one of which is a public key to encrypt the data, and the other is a private key to decrypt the data. When transmitting data, both parties must share the public key that can be used to decrypt the data, and the private key is confidential to keep it secret from others. Due to these overhauls, an asymmetric encryption algorithm can provide a higher level of security. Symmetric encryption often uses an algorithm with a key length of 256 bits, and a typical asymmetric encryption uses an algorithm with a key length of 2048 bits. In a payment system, data can be transmitted between the client and the server through symmetric encryption using the predefined shared key and can also be changed by using asymmetric encryption mode. There may yield a situation in which an attacker is capable of gaining access to the key of the symmetric algorithm. This is an inevitable condition if the attacker has access to the running process and system of the server or the client. This will never happen in the case of asymmetric encryption. Besides someone determining the key for an asymmetric encryption facility, the security of the method shall be compromised.

Tokenization Techniques

The above technique can be used to minimize the exposure of sensitive payment data. The sensitive data or payment account number gets replaced or tokenized with some format preserving a unique identifier. A token is an alias representing a record of the original sensitive data. It may or may not belong to any entity in the system. A token might be cryptographically generated using strong algorithms. In the payment context, the essential hallmarks of tokenization (as a security control) are as follows:

- It can result in irreversible or one-way transformation from the cardholder data to a token.
- The tokens used in payment exchange transactions cannot be reverse transformed back into the original value of the sensitive data. The tokens used in the payment authorization and capture process with the merchant or service provider cannot be used to recreate the sensitive data.
- It does not provide any additional information that might facilitate an adversary in their attempt to use cryptographic algorithms and lookup tables to divine the value of the original sensitive data.

Tokenization does not shift the data or payment cardholder details to a different location for storage or processing, nor does it change the system that uses the sensitive data or payment cardholder details. Tokenized cardholder numbers can be tokenized to complete transactions within that environment of functioning. These characteristics can be useful to meet compliance requirements. Tokenization reduces the scope of the compliance controls. Tokenization reduces the volume of sensitive data that directly supports banking, financial, and payment transactions. Tokenization can offer faster compliance audits with increased security. The implementation of the tokenization technique in the systems increases security and minimal trust assumptions. For example, if we are transacting with both legacy and tokenized processing, the existing legacy systems must also comply with the same rule. Format Preserving Tokenization tokens cannot contain the username, cardholder name, or card expiration date, and will be unrelated to the username and other identifiable information. There are many approaches to making the token value cryptographically correct, and the logic used to implement this is one component of a token vault.

Secure communication protocols

In the numerous transactions that occur online each second, the confidentiality and integrity of the data are of paramount importance. Entrepreneurs have the essential task of understanding what transactions their organizations are engaged in and the security mechanisms involved in safeguarding these transactions. Every online transaction is an exchange of information between a client and a server. Each online transaction should ideally be secured from eavesdropping, alteration, or unauthorized access. Using a secure communication protocol for online transactions would allow the client and server to assure the privacy and authenticity of exchanged data by encrypting parts or all of the communication. A secure communication protocol involves a number of technologies, from cryptographic algorithms to heavy-duty server software services.

The latest version of that protocol comprises improvements. It operates by encrypting the traffic between a client and a

server, guaranteeing confidentiality and integrity. The server's identity is theoretically confirmed by a Certificate Authority in the phases of alert and change cipher and is indicated in the third phase of the certificate. Though many details grapple with the connection between a client and server in these phases, this is enough to demonstrate that a server attempting to impersonate another can easily be signaled by a client since the server is able to confirm its identity. A trusted provider is a company that has its root certificate installed and is distributed with the standard web browsers. It is critical that the installed root certificate is up-to-date, as certificates expire. Such updates are not in the hands of the merchant but of the browser provider. It is thus also critical that the technical protocols be up-to-date, as the outdated ones are procured and therefore not secure. Furthermore, I would also like to highlight the benefit of several added security protocols and systems that might be used alongside in order to further secure financial transactions or a financial application, for example, making use of secure APIs or encryption technologies, some of which already meet or exceed encryption standards.

The use of insecure communication protocols may lead to several security weaknesses, some of which may be employed by criminals for payment fraud. As an example, if you were to install the client-side fraudster tool alongside a trojan, it is almost always possible to bypass the verified by enrollment process. We have seen a few cases where such attacks were successful even on verified enrollment APIs. If a server is outdated, it might allow for the use of a weaker encryption system, a fraudulent attack that can escape unnoticed because the user will see the padlock. Strong curvatures of such a protocol and non-tampering, in other words, verified by enrollment APIs on the client side often go a long way. The following are real-world examples of the use of secure communication protocols within financial applications. The use of secure communication protocols in transactions for card acquiring allows for authentication of cards, as well as for server certificates to authenticate payment gateways to acquirers. Server certificates allow for merchant and Payment Service Provider clients to authenticate the payment gateway from the client side. Additionally, a secure IP link using a certificate is another use case for an e-commerce application to authenticate its internal communication. Secure communication protocols are thus a requirement in order to assure that financial transactions can be trusted. Ensuring the payment application or financial infrastructure is properly designed and thus robust against criminal attacks is a serious matter. Other secure measures should be implemented on risky payment gateways, for example.

Authentication mechanisms in payment systems

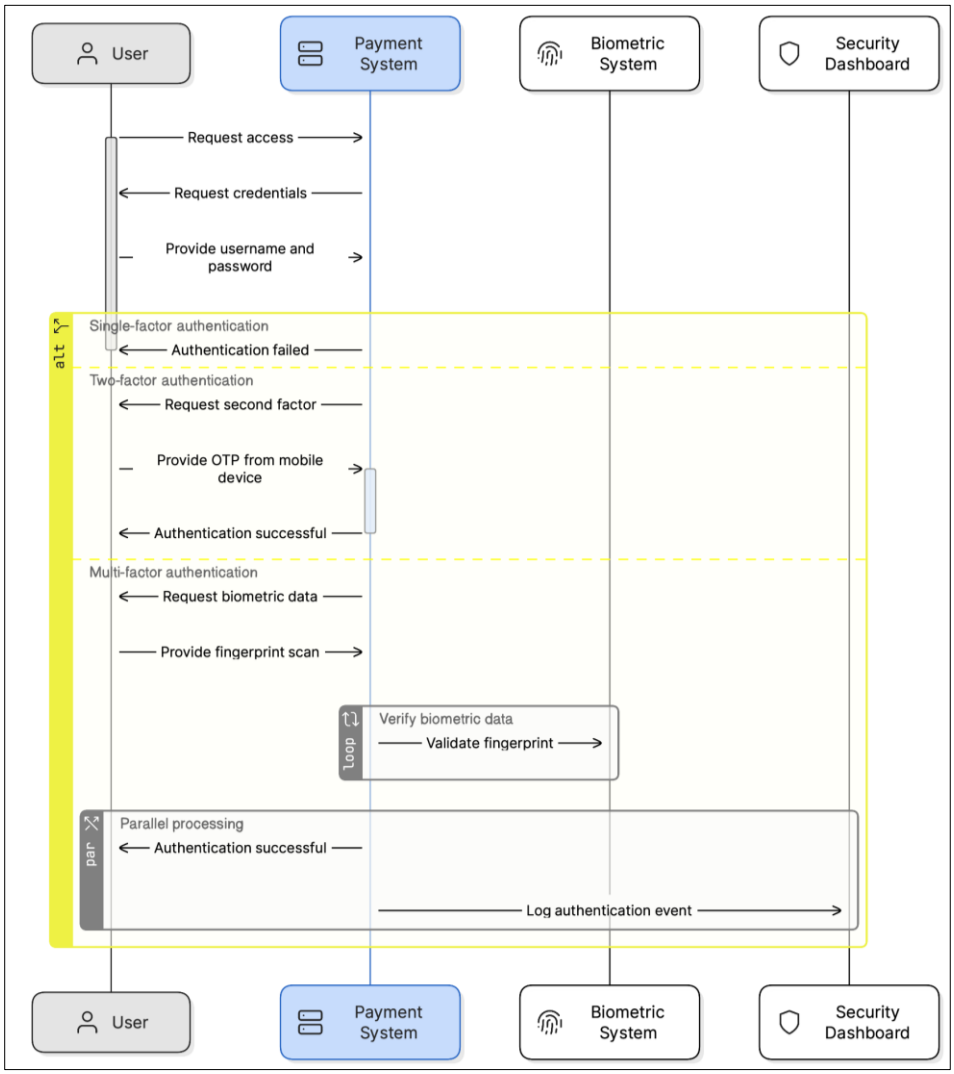

Fig 2: Authentication Mechanisms in Payments Systems

In order to place payment system security in context, it is important to be familiar with several basic secure payment concepts. For instance, to verify that the traffic matches traffic from a predetermined user account, payment systems typically employ an authentication mechanism that verifies the user's identity. Proper authentication is an essential line of defense against increasingly sophisticated, multi-faceted security threats. Traditional methods for verifying user identity in a single-factor approach, such as usernames and passwords, are becoming increasingly ineffective protection mechanisms. This has resulted in the widespread acceptance and increasing popularity of two-factor authentication, which requires a user to provide two sets of evidence, such as a username and password.

Along these lines, multi-factor authentication necessitates a user to provide multiple authentications. A typical MFA scenario authenticates by combining what a user knows (a personal identification number or password), with what the user possesses (a security token, a mobile phone), and finally what a user is, as determined by some sort of biometric verification. This combination makes illicit access to a network much more difficult. The last example of "what a user is" is often referred to as biometric identification or biometrics. It is defined as the field of studying how to uniquely recognize humans based on characteristics and traits of their anatomy. Biometric verification uses a unique physiological characteristic of an individual, based on personal body features such as a fingerprint, iris, voice, facial feature, or hand geometry. For instance, fingerprint scanner or facial recognition system, plenty of software products integrate a modern multifactor authentication system based on biometrics. But the reliability of biometrics is still going to face many challenges, both technical and non-technical, such as legal, social, and privacy issues. In addition, the acceptance of biometrics by end-users remains the biggest challenge. Technology performance should be discussed with user acceptance. From a technical standpoint, it is important to recognize the roles played by observers, impostors, and legitimate users. Furthermore, the long-term static characteristics that remain relevant over time should be validated for the biometric data input. In various circumstances, it is considered that such static biometric characteristics may have poor user acceptance potential and represent a security issue. Among others, several efficient biometric authentication methods are already widely used, such as fingerprint recognition, facial recognition, and iris recognition. Biometrics could become the most dominant authenticator for payment systems, playing another vital role in the security of payment systems.

Multi-factor Authentication

As already mentioned above, MFA is a powerful tool for enhancing security used in payment systems. Unlike a single password, using MFA requires users to provide at least two pieces of evidence to prove that they are who they say they are. There are typically three types of factors that could be used in MFA: knowledge-based (what you know); possession-based (what you have); and inherence-based (what you are). Examples of “what you know” include passwords, PINs, or patterns, while examples of “what you have” are SMS codes, email codes, authenticator app-generated codes, and hardware tokens. Examples of “what you are” include biometric features like fingerprints, faces, voices, irises, keystroke rhythms, gait, or signatures. Any combination of these factors could be used. However, all U.S. payment service providers are required to implement at least two of these factors—passwords and any other knowledge-based device supported by the customer—for accessing accounts via end-user digital channels or initiating transactions from the customer’s digital channel to or from the payment service. The use of MFA, also known as “strong” or “risk-based” authentication, is intended to increase the security of customer data and transactions, reduce the risks associated with compromised authentication, and mitigate the risk of entering into unauthorized transactions. The belief is that financial institutions that implement MFA could prevent unauthorized access to customer accounts immediately and limit the risk of data losses in case access is approved by an unauthorized party. The use of MFA can also help to reduce the risk of identity theft when used in customer authentication and for the detection and prevention of new account fraud before a suspected party could unduly warrant. But despite these advantages, the use of MFA also confronts some challenges such as complexity, privacy, and user experience. The use of some of the technologies for MFA, including cell phone possession, has raised questions [2 3].

For the financial sector, the use of MFA envisions the use of personal biometrics (what you are) for confirming payment operations. However, remote and in-person (bricks-and-mortar) use of biometrics differs significantly. A general guideline in assessing biometrics for secure, high-risk payments might be that, as a “golden rule,” personal biometrics do not scale well. This is to say that when the number of interacting and authenticating bank customers increases by an order of magnitude, banks could be more attractive to imposters. Judging biometrics from this angle, a way forward might then be, when presented with biometric options, to consider a lowered acceptance of payments as a protective tool for keeping the entire ecosystem secure. Best practices in promoting biometric information protection might then include a carefully drawn plan that provides auditors with evidence that security rules are in place and are being followed. This might include secure biometric template transfer, storage, and matching, as well as the use of biometric encryption alongside symmetric and asymmetric system checks. This way, it is possible to work toward the envisaged high-security identity platform, improve understanding, and gain user acceptance. A cornerstone for security in the upcoming financial regulation setting could include secure and privacy-protecting biometric/behavioral information. Further, the use of MFA brings increased alert levels at various touchpoints within the bank, making the bank more capable of detecting potential fraud. The alert-level dashboard will serve as a near-real-time monitoring tool that provides a comprehensive view of any fraud occurring at the bank. Integrated solutions would help to identify root causes and protect against any possible intrusions in the future.

Biometric Authentication

Biometric authentication is a fundamental departure from traditional systems, which rely on "what you know" or "what you have." The user of a system verifies his or her identity based on a biological or behavioral characteristic. Several biometric modalities include: Fingerprint scanning – This method requires the measurement of some ridge/valley structure within the bulb of a finger in order to identify an

individual. The scanning can be passive, active, or even touchless. Facial recognition – Its methodology is based on "static" or "dynamic" structure, where the former relies on the physical structure of the face, the shape of the features, and the distance between the eyes, among others, and the latter relies on "likeness" such as measurements between the face and facial features. Iris detection – Our iris is a unique, visible disc-shaped structure in the eye. Its pattern is formed during the third trimester and remains constant throughout life.

During system enrollment, the user is invited to provide a biometric sample. The system extracts the unique features of the original sample and converts those features into a template. This template is essentially a data file that represents the unique features of the biometric sample. This process is irreversible, and the original sample can never be reconstructed from the template. However, if the original sample is re-presented, the enrollment process will generate another template that, if compared with the original, will verify the identity. Thus, the first function of the template is to allow the system to remember the user. Once the system knows who the user is, it can provide secure access or perform secure transactions. Some fraud scenarios using biometrics could include theft of biometric data. Fingerprint smudging attacks are an example of possible vulnerabilities: If an attacker obtains a fingerprint sample, he or she can use it to authenticate a biometric sensor in the second factor. If the biometric key is also stored on the device, then the attacker is essentially adding a second identity factor. Many consumer devices today – particularly smartphones – also use some kind of biometric identity system, with most using fingerprint programs.

Possession of such devices could be accounted for non-repudiating transactions. Biometric systems raise both privacy and data protection concerns. It is imperative to have stringent governance frameworks to regulate the use of biometric data in payment systems. This is particularly important given the high level of counterfeiting, unauthorized use, and identity theft in the field of digital payments today. Furthermore, implementation of biometric authentication depends on proper implementation, vetting, and storage of biometric data. As with any digital system, it is neither invulnerable to hacking nor foolproof when it comes to accurately identifying users. False positives can occur, meaning a biometric system scans a user's biometric incorrectly, thus not allowing access to the user. Furthermore, biometric systems are only as secure as the repository for user data. A data breach, therefore, can theoretically act as the "one-two" combination to access all user accounts. Payments can become truly tokenized if a new crop of startups develops stronger biometric authentication processes. Combining this authentication with the creation of a digital identity system that is feasible, usable, and agreeable to users is a daunting but not impossible task. Biometric scanning will become integral to finance sector security. A robust governance framework is a prerequisite to the deployment of any kind of multilateral authentication, be it biometric or another kind of fully user-prompted and controlled technology. It would ensure a solid set of rules, roles, and rights for acceptable use [4].

Security measures for mobile payment systems

Mobile payment system security must evolve in light of the relative newness of the mobile payment space and new techniques, technologies, and targets that are aggressive and ever-evolving. The mobile payments market continues to grow in adoption, with providers seeing substantial increases in both the user base and the average mobile payments amount. However, with the rise of convenient and attractive options come additional and enhanced risks. With growing offerings, the opportunities for fraud to present themselves are also increasing. To mitigate these threats, security strategies and new systems must be tailored to the specific characteristics of mobile payment systems. Some key methods of ensuring secure payment system development are adapting and observing secure coding practices and developing systems that include both hardware and software encryption.

Experts in the mobile payment security industry face a variety of issues in mobile payment system development. One such issue of great importance is that of a secure mobile app. From a conceptual standpoint, implementing a secure mobile commerce app entails developing a regular web or desktop web commerce application, followed by extensive security testing and validation of the app. From the business or security perspective, this core concept does not change. There exists a gamut of security testing methods. Additionally, the client itself is susceptible to attack. On the upside, entities have been developing standards for the development of a secure mobile app. A well-adhered-to industry standard is provided by recognized organizations. These organizations provide a wealth of information and tools to aid in the development of secure software, with an entire project devoted to secure mobile app development. When the onus for secure software is not on the developers, it is placed on the end user. A standard demands that its customers ensure standards of security. This standard demands that systems are in place to ensure user education with regard to the defense of their system. Particularly due to the state of mobile technology, the malware potential of untrusted and unknown programs being downloaded from app stores, end-user education and training is extremely vital when it comes to a secure mobile payment environment. Furthermore, developers of mobile payment applications and organizations that offer mobile payment methods should be concerned with adhering to the payment security standards that exist. Recognized services have all created their own standards for payment security [5].

Conclusion

The security of digital payment systems hinges on a combination of advanced technologies, regulatory compliance, and user-centric practices. Encryption and tokenization remain foundational to protecting transactional data, with symmetric encryption enabling efficient secure channels and asymmetric encryption ensuring non-repudiation in untrusted environments. Tokenization minimizes the exposure of sensitive cardholder data, aligning with compliance mandates like PCI DSS. Authentication mechanisms, particularly MFA and biometrics, provide robust defense against unauthorized access, though challenges such as user acceptance and data privacy require ongoing attention. Secure communication protocols like TLS are indispensable for maintaining data confidentiality and integrity in online transactions. As mobile payment adoption grows, secure coding practices, hardware encryption, and user education are critical to countering emerging threats. Future advancements in biometrics and decentralized systems like blockchain promise enhanced security but

demand rigorous governance frameworks. Ultimately, collaboration among stakeholders in financial institutions, regulators, and consumers is essential to fostering a resilient and trustworthy digital payment ecosystem.

References

1. PCI Security Standards Council. PCI DSS v3.2.1: Payment Card Industry Data Security Standard. 2018.
2. Daragmeh A, Lentner C, Sági J. FinTech payments in the era of COVID-19: Factors influencing behavioral intentions of 'Generation X' in Hungary to use mobile payment. J Behav Exp. Elsevier; 2021. Available from: https://www.sciencedirect.com
3. Najib M, Fahma F. Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium … Int J Adv Sci. 2020. Available from: https://www.researchgate.net
4. Datta P, Bhardwaj S, Panda SN, Tanwar S. Survey of security and privacy issues on biometric system. In: … and Cyber Security. Springer; 2020. Available from: https://www.researchgate.net
5. Nurgalieva L, O'Callaghan D, Doherty G. Security and privacy of mHealth applications: a scoping review. IEEE Access. 2020. Available from: https://ieeexplore.ieee.org.