Deep Science Publishing
https://doi.org/10.70593/978-93-49910-78-2_6

DeepScience
Open Access Books

Chapter 6: Advanced techniques in securing payment gateways and transaction networks

6.1. Introduction

Retailing and e-commerce are presenting subjects of many researches in security. In the retail business area, after giving a cashier to the customer, a retailer will be obliged to accept any payment that was consecrated as legal tender according to the country laws. Therefore, the cashier is the point of collection of money, and the connection between the customer and retailer. The cashier is representing the importance of payment; therefore, all actions of merchants and customers, related to the payment, are sensitive and have to follow security constraints for creating trust in both sides. The customer has to be sure that the retailer is not collecting money without performing the required service and the retailer has to be sure that the customer will not enable fraud without guaranteeing money payment (which is a basis of trust). These actions are generally called transactions. Security aspects, in general, apply as well in the e-commerce area for securing transactions (Liu & Li, 2022; Chowdhury et al., 2025; Hossain et al., 2025).

Concerning transactions, the current paper presents aspects related to transaction assurance in networked environments, without which trust cannot be created and finally security cannot be created. The general activity of delivering a product or service in exchange of money can be viewed in a more complex way, but at the base, it contains the transaction. In accordance with the Webster Dictionary, a transaction is a business or occurrence involving two or more parties that have some effect upon at least one of the parties to the business or on some property that is owned. Related to networks, the transactions are electronic transactions. In the e-commerce area, each transaction occurs in the cyberspace when the customer places an order in a web-based application, clicks on a button, and transfers the order for a payment (Wang, 2023; Yamini et al., 2023).

6.2. Understanding Payment Gateways

The term "payment gateway" refers to a company that acts as a conduit between buyers and sellers by accepting the credit cards or other electronic payment systems of buyers and transferring the information to an acquiring bank for transaction approval. It is analogous to a broker that facilitates financial transactions. Payment gateways are specialized for a vertical market. For instance, they may restrict payment options to credit cards from only one country or unique group or package. Payment gateways may also specialize in keying transactions over the internet or via fax on behalf of businesses without on-line or card-not-present credit card services. Payment gateways are essential components of any e-commerce endeavor because they facilitate electronic transactions over the internet. There are many online payment gateways, which are deployed by shop owners after opening a merchant account and establishing non-refundable deposit/transaction fee terms.

Payment gateways transmit authorization requests from a merchant's server to the cardholder's bank for verification and then transfer the response back to the merchant for transaction completion. Payment gateways are specially designed for a specific industry niche and to satisfy certain regulatory requirements specific to that vertical market. Payment gateways may cater to only one mode of payment or services from only one particular government. Payment gateways are usually keyless and are used by mail-order and telemarketing businesses, facilitating authorization requests made without the benefit of a physical card and cardholder.

6.3. Threat Landscape in Payment Systems

As payment systems progress, so do the threats associated with them, both in terms of the increased volume of attacks across all sectors and their complexity. They have shown exponential increases over the last decade, both in terms of volume, complexity, as well as in the damage inflicted upon businesses by ransomware attacks, data breaches, customer account hijacking, cross-site scripting, code injection, point-of-sale attacks, investment fraud, and business email compromise. Payment-related industries such as banking and finance, retail, and telecommunications experienced the highest number of breaches. Over 3,000 security incidents related to the Payment Card Industry ecosystem were reported in 2021. Payment card skimming has also increased, with payments fraud reporting from the card brands continuing to show it as a significant problem.

Cyber attacks that target money, payment, and payment-related sensitive information for illegal gain are created and leveraged by cybercriminals, which motivates their attacks over all other attacks. Financial data is the second most-aimed for data breach record in the InfoSec community when broken down into industry and sector.

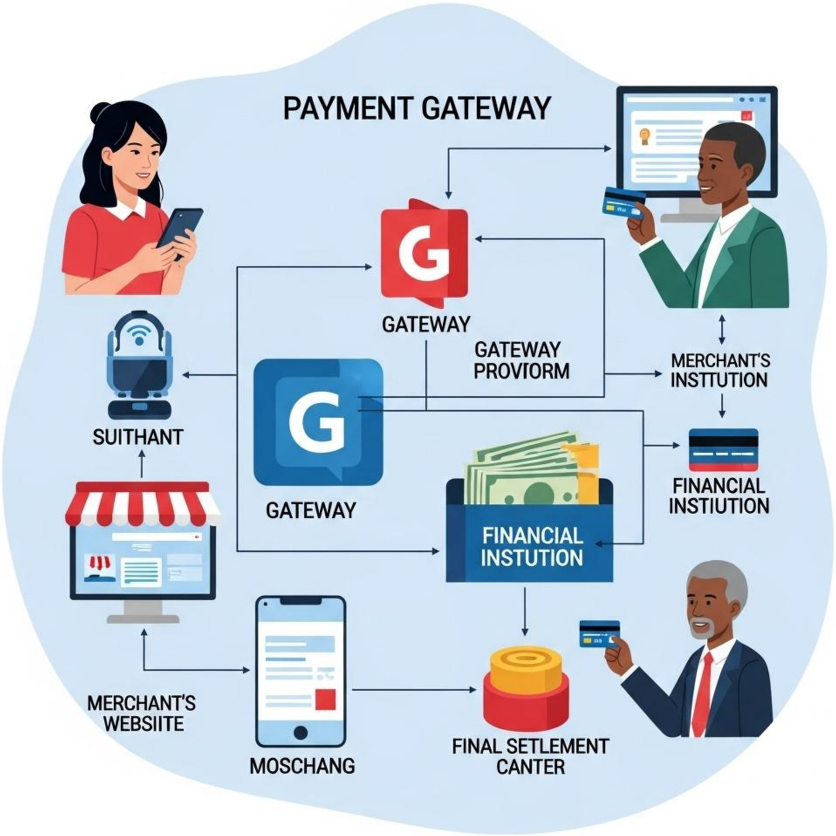

Fig 1 : The Flow of a Payment Gateway Transaction

The oldest and most-known method for such theft is credential theft, where attackers capture and later reuse the login credentials for a payment or banking account in order to freely transfer money and information, in effect impersonating you. However, cybercriminals have since developed techniques such as spear phishing, deep URL compromise, remote access Trojan, injection malware, and various simulated social frauds that can cover the last mile of the attack chain and allow for success. More sophisticated attacks such as data breaches involving backend data scraping or exploitation of security audit failures target sensitive payment application controllers that handle the invention’s payment information for wholesale amounts of sensitive financial data.

6.3.1. Types of Cyber Attacks

The types of cyber attacks that a payment or retailing system may be the victims of, or which may target it, can be classified in several ways. The most common ways of classifying them pertain to the stages of the transaction process they target, and to whether there is a malicious motivation or not. A cyber attack on a payment gateway or system can be either a financial fraud attack or a cyber-crime based on an Actual Service Attempt. When the attack is malicious and has a profit-seeking motivation, it can aim to affect either the payment gateway payment service process or the associated payment network transaction process – thus being characterized by the motivation of defrauding one party to the transaction or both parties. When there is no malicious motivation, on the contrary, the Actual Service Attempt target can be considered either the payment system gateway, payment service or payment network transaction – without any fraud seeking action but with the intent of an attack on the confidentiality, integrity or service availability of any payment processes.

Several versions exist regarding the classification based on Steps of the Transaction Process and Malicious Motivation. The two schemes may belong to different categories since the first one states that there is a fraud attempt and does not consider the motivation of the action, while the second asserts a motivation. No omnifying taxonomy of attacks exists, part of the complexity being due to the enormous variety and dynamism of technological based solutions that these days are used for transactions in the payment process. And by the equally and even more rapid variability of the methods of frauds or crimes used by malicious people, that often target the new offerings.

6.3.2. Emerging Threats

Emerging threats related to e-payment and transaction authentication techniques face upcoming challenges for user authentication techniques in payment services. Accounting for security objectives in electronic transactions across the globe, standards on security in electronic payments consider authentication techniques during payment services, specifying levels of assurance. However, the increased adoption of mobile payments and related payment applications such as digital wallets are accountable for breaches and fraud by criminal organizations, with threats linked to authentication. Application Providers are entrusted to deliver Secure Applications and Related Services, that focus on the form and logic of the application itself, including guidelines for trusted system components and the application lifecycle. Security Mechanisms and Assurance are generally based on susceptible areas in mobile devices categorized in device protection, application protection, cryptographic protection, voice transactions, and biometric protection. Cyber Security assurance must fit and cover security service levels of biometric authentication methods, as complying with the ePayment Fraud challenge to balance security, user experience, privacy, and customers need for superior usability.

Trust Services in e-ID are required to complement the recent high-speed growth of e-payment transactions aiming at fraud prevention. Assurance areas are driven and specified by the Trust Framework for entities acting on behalf of a credentialed entity. Also, Device ID is a liaison in association with other transaction items such as account linked and location linked items to prevent fraud. eID and Related Services for Authentication and Identity Assurance are exposed to several attacks including man-in-the-middle, phishing, malware, replay, and session hijacking namely. As service level assurance increases over time, eID, ePayment, and eBanking technologies may become increasingly scrutinized toward a generalized, all-covering trust service solution. Thereby guaranteeing that all authentication and identity validation services which are lawful in the target area and also able to operate securely and supervise trustworthy user transactions across business processes.

6.4. Cryptographic Techniques

Cryptographic techniques are the state-of-the-art solution for ensuring anti-spoofing, non-repudiation, authenticity and confidentiality on transaction networks. Non-repudiation assures the parties involved in any transaction cannot deny the existence of the transaction. Non-repudiation is usually provided with public key algorithms or hash functions combined with public key algorithms. Public or private key/asymmetric algorithms can be used to ensure non-repudiation, confidentiality and authenticity when transacting sensitive data. Commercially available digital signatures and encrypted format are often adopted. If all parties in transactions are required to keep data confidentiality over digital signatures to ensure authenticity, then a symmetric-key/hashing technique is needed for the sensitive data. Digital signatures can be used to authenticate required keys to ensure data confidentiality. Data authentication and integrity can be assured securely via a hashing function along with the private key with an available public key.

API or dedicated hardware for cryptography is made available by commercial chipset manufacturers to reduce the cost and time implementability for products adopting secure authentication. Designers can rely on provably-secure algorithms for achieving confidentiality, data integrity, and authenticity, and so on, based on sound knowledge in the selected algorithms. No matter which operation mode is applied in using a block cipher, the algorithm has to be implemented properly. In addition, those cryptographic functions cannot ensure security alone; secure provisioning of keying data and a quality user interface are also critical for the overall effectiveness of security. A best practice for key provisioning and a secure user interface are usually referred to as key management and user interface management.

6.4.1. Encryption Methods

Encryption is the first cryptographic technique. It renders plaintext unreadable to unauthorized parties, but allows the authorized parties to recover the original plaintext. Similarly, a digital signature for an original plaintext allows any party to verify that this is indeed the original plaintext, while no parties other than the signer can create different signatures on the same plaintext. A digital certificate allows any party to check the ownership of the public key of the signer, thus vouching for the identity of the signer. The two primitives, encryption for confidentiality and signatures with certificates for authenticity, together can be used to provide the stronger guarantees about modern communications provided by cryptographic techniques.

The most important of the symmetric ciphers today is the Advanced Encryption Standard (AES), which was adopted as the federal encryption standard for the United States in 2002. The AES is a symmetric-key block cipher with an expanding key size of 128, 192, or 256 bits, and the block length is 128 bits.

The most important of the asymmetric ciphers today is Pretty Good Privacy (PGP), which was invented in 1991 and has grown into a family of standards and commercial software products. The original purpose of PGP was to enable the secure sending of messages. The original PGP itself used security keys corresponding to RSA for encryption and digital signatures, and used the IDEA block cipher to provide confidentiality. The public key operations of RSA are too slow to encrypt larger amounts of plaintext; thus, PGP was primarily a message encryption and signature system, working with file and email messages.

6.4.2. Hashing Functions

A hashing function is based on a one-way compression function which maps arbitrary-length data to a fixed size, i.e., a hash value. The hashed data can be uniquely identified by a unique hash value for a unique input. Ideally, the hash values of two different inputs should not collide. Furthermore, given a hash value, it should be infeasible to find the input that generated the hashed value. If corrupted data is fed to the function, its hash value displayed during computation should change, indicating that data has been corrupted. A hashing function is applied to each transaction data consisting of sender information, receiver information, data amount, and data type. The encoded image is stored in a database, along with other encoded data that is useful in decryption. The hash values generated for the transactions of two users should not collide, i.e., different hash values should be generated for different transaction data.

If the transaction is sent to a particular user, the hash value is stored along with other transaction data that an authorized user can access, such that even if the hashed transaction data is changed by another user who does not have access, a different hash value will be generated. The unique properties of hashing function make them useful in a proof of receipt. The user who sends the receipt after performing the transaction first concatenates the sender, receiver, and the amount paid in the receipt, such that the intended transaction has received and edited. The user who receives the proof can decrypt the encoded value using the unique private key of the sender and compare it to the hash value generated from the decrypted receipt content. If the two match, it is proof that the receipt has not been tampered with; if not, the sender should resend using the property of collision-resistance.

6.4.3. Digital Signatures

Public Key Cryptography provides practical ways of guarding against each of these frauds with the use of Digital Signatures. A Digital Signature lets a server make a statement that is verifiably authored by the server. The user can then trust the information, knowing it was placed there by the author and has not been altered since. A Digital Signature could be used to sign an authentication protocol. While that would protect against a spoof attack, the use of plain Digital Signatures would not stop the session from being entered into. In combination with a shared secret between the server and the server computer, however, Digital Signatures provide mutual protection against both attacks. A Digital Signature algorithm provides a keyed or unkeyed hash function and the secret key used to generate and verify the Digital Signature is effectively a session key shared only between the server and the customer. The user mixes the session key into the message to be signed, thus preventing someone from using the Digital Signature later to convince a bogus session computer that it is the right one.

Digital Signatures are produced with the following algorithm, which effectively creates a secure keyed hash function. Key Generation: the server creates a pair of keys, the private key kept secret and the public key distributed to anyone authorized to interact with the server. Key users are typically involved in a manually-entered or protocol provided handshake Phase 1. Key Sharing: the two potential key users agree on a session key. Phase 2. Digital Signing: the signing user creates a hash of the message to be signed and hashes the session key into that hash. The user encrypts the resulting hash with the private key. Phase 3. Signature Verification: the verifying user hashes the message being signed and hashes the session key into that hash. He decrypts the previously encrypted hash with the public key. If the two hashes match, the verification is successful.

6.5. Authentication Mechanisms

Authentication verifies the identity of users and applications accessing a network or online service. Authentication is required before granting access to confidential data or performing secure tasks such as making payment transactions. It includes items such as ensuring that a website a user is visiting is genuine and not a fraud website attempting to pass itself off as a legitimate one, and it includes mechanisms for ensuring scammers cannot impersonate a legitimate phone number to obtain sensitive information from users. Proper authentication mechanisms protect users and authorized applications from unauthorized actions and data breaches.

Involvement of multiple parties in transactions and the online movement of financial data reduces control over authenticating users and performing actions. The nature of the virtual environment and the open access model make verification of signing parties a challenge that is often faced with simple security measures like passwords, which based on prior statistics have, aside from being insecure and easily guessed, been proved to be insufficient for protecting even the most critically sensitive databases. The fact is that users often forget their passwords. They make them simple or reuse them for multiple accounts, thereby exposing themselves to breaches of sites where there is less concern about password theft. Moreover, an attacker can easily guess or steal a user's password using social engineering or malware. Even with these reasons for not relying solely on passwords, many websites continue to use them alone or in conjunction with security questions, leaving users vulnerable to severe damages.

6.5.1. Two-Factor Authentication

Two-factor authentication (2FA) requires two different authentication factors, namely something the user already has and something the user knows. 2FA is widely deployed. For example, ATMs require the user’s debit card plus a PIN. In most cases today, the first factor is a mobile phone and the second factor is a password or PIN. First, the user logs into the service with username and password. Then the service uses an SMS service to send an SMS to the user’s mobile phone that contains a secure code. The user inputs the secure code, which the service verifies. If the secure code is valid, the user is allowed on the service. Many connected systems do not yet use 2FA. For example, a payment gateway may allow an e-commerce website to connect for communications without using 2FA. This means that an attacker could create a fake e-commerce website and connect to the payment gateway to intercept all transactions between a customer and the real e-commerce website.

Some services allow the use of a mobile application that generates a short-lived code that the user has to enter as a second form of authentication. The advantage of this mobile application-based authentication is that it does not depend on the SMS service. The ability to use mobile authentication is still relatively rare in many Internet services and requires the use of a specially-designed mobile application. Some services will even provide a special mobile application that runs on a separate device, such as a company-issued smartphone.

6.5.2. Biometric Authentication

A rapidly growing area of research is the authentication of users using biometric indicators. Simply explained, these indicators are ones inherent to the individual user and unique to that user, such as a fingerprint biometric or a feature of their iris. The area is becoming popular as an area of research and development for a number of reasons. The most compelling is that on the one hand it is quite convenient for a user to authenticate to a system without the necessity of remembering secret passwords or carrying tokens, but on the other hand research into biometrically matching at high speeds has progressed to the point where a biometric-related authentication mechanism can cope with the speeds and flow of traffic typical of a payment gateway. The clear advantages in implementation of biometric authentication means that a payment service provider can raise the level of trust in the payment gateway without any significant impact on the end-user.

However, this is not to say that there are no concerns related with accommodating an individual’s biometric. Storing and maintaining the biometric information necessary to support this is a very different challenge than storing and maintaining a password or token. These concerns, along with the concerns of privacy and data security in general, have significantly slowed the adoption of biometric authentication into public use. However, it is a safe bet that it is just a matter of time before these technologies overlap. In addition, implementations of authentication systems using biometrics have the very major advantage of reducing the cost to a payment service provider of managing the client-side aspects of an authentication system, since operators of services provided by the payment provider now don’t have responsibility for maintaining the integrity of credential information such as passwords. Biometric authentication is an area of active research and discussion is ongoing. The consortium with the governing body over how the data associated with a biometric authentication ought to be expressed has recently published the standard that defines how such information ought to be built.

6.5.3. OAuth and OpenID

Federated identity schemes allow users to log into multiple applications across different domains with a single password (or some other authentication credential). Such single sign-on solutions can reduce the number of passwords a user must keep track of and can enable a user to access many different online resources with a single credential managed by one of those providers. In addition to the benefit of easier-to-manage user credentials, reducing the number of credentials a user must manage can also reduce the occurrence of password reuse across domains, thereby mitigating a significant source of vulnerability when a specific domain is hacked to expose the password hashes.

OpenID was one of the first Internet-wide federated identity solutions, and a number of OpenID providers appeared to allow users to get OpenID credentials. One of the most well-known providers became a major tech company, which attracted a large number of users. Because accounts can be used to access various services other than OpenID, users can often perform additional actions after losing access to the OpenID, and rely on this association for additional security. However, in recent years, OpenID has started to fade, somewhat, in popularity and usage. Certain exchanges originally interacted with OpenID providers to allow clients to log in using their OpenID credentials. The decline of these exchanges may have contributed to the decline of OpenID. Currently, OpenID is not an identity service used with many of the popular services, and others primarily offer OpenID as a service supporting extension to enable login for users who still wish to use OpenID.

6.6. Secure Socket Layer (SSL) and Transport Layer Security (TLS)

SSL offers multiple levels of protection. It provides network security during transmission, making it impossible to eavesdrop on a session or hijack any session data while in transit. SSL is used to authenticate the data source. An SSL-secured web page can only be established by the server named in the certificate and only that server can read the session data after its transmission. SSL secures data integrity, ensuring that the data is not altered in ways that go unnoticed. If the data is modified, the change is detectable.

Transport Layer Security (TLS) is the next generation of SSL, providing the same security, though with an improved security performance. Like its predecessor, TLS is an encryption protocol that protects data transmitted between two parties over TCP. TLS records are used to encapsulate different types of protocols. TLS is not more complex than SSL; it is disjoint from SSL in some ways, and more complex in others. While the two protocols are nearly identical, there are certain key differences: they use different types of session IDs; the negotiation messages are somewhat different; TLS can use any MAC algorithm, not just those defined in RFC 2104. There are also differences in error alerts of the two protocols. For example, TLS uses a warning level alert to signal that the connection has been compromised, as in when a warning level alert is used by SSL. Unlike SSL, TLS does not feel the need to define an alert for unknown messages;

implementations simply ignore any alert that they do not understand. Finally, the majority of TLS MACs replace the MD5 MAC used in SSL with SHA-1 or whatever algorithm is defined in the message digest pseudo-random function. TLS is the IETF standardization of the SSL 3.1 protocol.

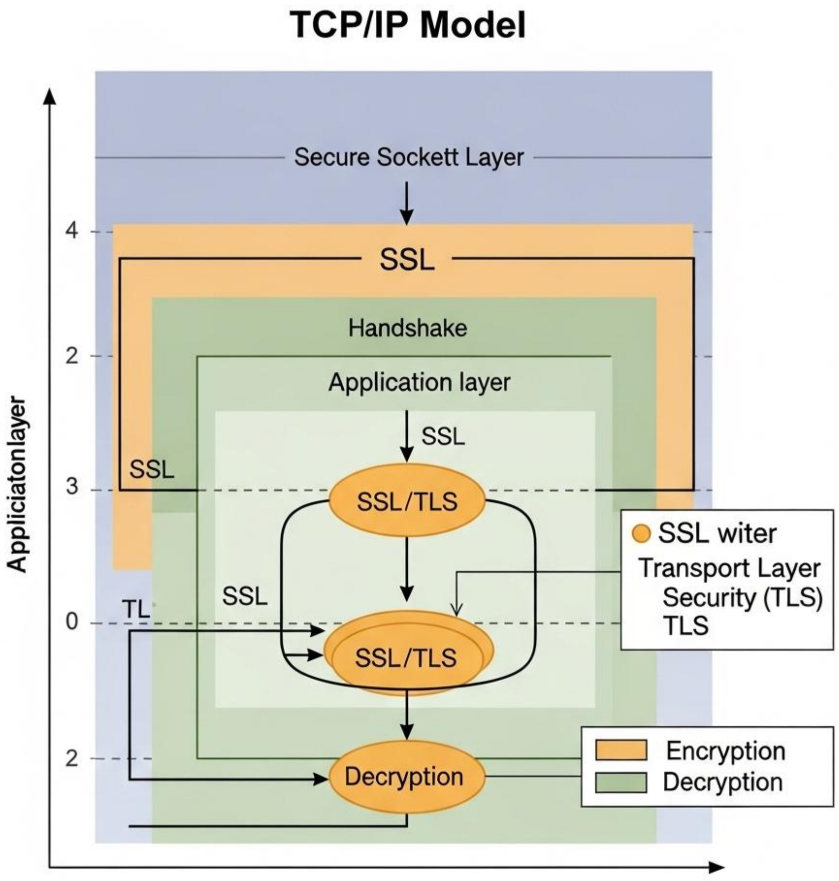

Fig : TCP/IP Model

6.7. Tokenization and Data Masking

Data protection is a task that covers multiple domains. It is necessary not only to buy a physical device to protect your network, but also to use certain techniques and store the data in such a way that it is not useful or helpful to malicious entities. Different specialized techniques can be used to protect large databases that process highly restrictive data, such as databases related to payment processors and financial entities. Tokenization and data masking are two of these techniques.

Tokenization is the process of creating a token that replaces sensitive data. These tokens will always be unique for the original pieces of data, but do not disclose any informative content, other than being unique. Data masking, on the other hand, takes the original data, transforms it during the process such that it cannot be reverted, and stores the new data. The significance of this new data only resides on possibly being read by a transform function associated with the database. The function that performs the masking cannot be stored as part of the database metadata, because this would help attackers that wish to reverse the process; it has to be an external entity. Later, the data will pass through a verification step to determine if it is sensitive or if it can remain in a database without requiring special security considerations. Tokenization, masking, and encryption have key roles in this process. Tokenization and masking attempt to substitute encryption by transforming the file permanently, while encryption is based on the use of encryption/decryption keys to perform the transformation at will.

6.8. Fraud Detection Techniques

6.8. Fraud Detection Techniques Fraud is an all-too-successful business model for many individuals. As customers move online, e-commerce has become a focus of increasing and very profitable criminal activity. Fraud detection for e-commerce is a massive problem, with literally billions of hypothesis tests conducted every day. Credit card and identity theft, online auction scams, aggregator site shopping scams, and much more are lucrative underground business. What makes fraud detection especially difficult in today's online world? Large data size: At nearly every e-commerce site, the data volumes are vast, from Internet fraud detection, which deals with predicting which transactions are fraudulent, to credit risk, which is primarily concerned with the rating and re-rating of consumers' likelihood to default on loans. Delicate imbalance: Consider a supervised learning problem where an online auction site is to be trained to detect fraud amidst its transactions. This auction site processes a very small fraction of fraudulent payments; e.g., suppose that out of 100 million transactions for an e-commerce company, only 40,000 transactions are fraudulent. Processing the task as any other binary classification task would lead to a model that would classify the vast majority of transactions as non-fraudulent, leading to an extremely high accuracy for predictions but a terrible classification model for fraudulent transactions. Most of the research in imbalanced binary classification has centered on network intrusion detection, emphasizing the corporate protections of the network.

6.8.1. Machine Learning Approaches

INTRODUCTION. The rapid growth of fraud on the Internet and the inexorable rise in payment transaction volume have brought a lot of attention to this area. Fraudulent payments cost the industry significant financial losses. The estimated loss in the online payment industry is about 120 billion dollars each year. Therefore, an increasing number of merchants are investing a lot of money in fraud detection devices. Fraud detection is an interdisciplinary domain. It inherits elements from various fields such as artificial intelligence, data mining, and machine learning. Credit card companies and online merchants are developing really-high-level fraud detection systems that can adapt to new fraud patterns. DETECTION BY MACHINE LEARNING TECHNIQUES. The exploding prevalence of fraud over the last few years has made it financially costly for payment gateways to prevent it. Merchants and customers have been suffering losses for online fraud. In addition, consumers have been unwilling to do online transactions because of the reputation from the news about data leaks over the Internet. It has led to an attempt to detect online fraud using data mining and machine learning techniques. Machine learning techniques are able to detect the characteristics of normal samples and fraudulent samples. However, the main challenge in this area is the density of negative fraud cases. Therefore, different approaches have been proposed to alleviate this problem and increase the performance of machine learning approaches. Initially, some approaches reduce the imbalance in the dataset. Data sampling can be divided into oversampling and undersampling. Some of these works applied a synthetic oversampling method to generate different datasets. Others attempted to detect fraudulent cases by clustering algorithms. Since clustering is not supervised, it is not possible to label the targets as normal or fraudulent unless a labeling step is used. Some approaches manipulate the data without any prior data sampling; they directly involve deep learning architectures.

6.8.2. Behavioral Analytics

To identify frauds proactively, behavioral analytics examines how consumers and merchants use their accounts, searching for patterns that, if altered, would point to possible fraud. When users are initially authenticated, behavior analytics can create a behavioral fingerprint that distinguishes true users from impostors when these users return. If an invalid user presented unique password information, continues to enter that same sensitive data on the login form, and despite the fact that normal users would be ineligible to change their passwords shortly after the password is created, the impersonator is forecast to be a bot. This method can apply to financial applications, where users log on daily or monthly to review their investment portfolios. A modeled risk associated with every user can prevent notice alerts from being produced for low-risk users on nonurgent days.

Behavioral analytics is a cascade of algorithms capable of being trained with the data from an authentication and intelligence system. Sensitive use cases and behavior patterns are developed and improved through careful combination and analysis of the data, but all of the fraud patterns must be established first. Furthermore, they still lack an effective way to define the characteristics of legitimate user behavior and map sessions to distinctive characteristics based solely on unique interactions. These characteristics cannot rely on a high number of interactions because behavioral analytics is a real-time system.

6.9. Regulatory Compliance and Standards

Payment gateways and financial service providers are obligated to adhere to various standards and regulations. We will mostly concentrate on the Payment Industry Data Security Standard in this section. Since the underlying principles of this standard address the secure handling of cardholder data, it plays an important role in securing transaction networks, where it is deeply integrated. Also consider the General Data Protection Regulation. It establishes regulations for the handling of data that could lead to revealing the identity of a person. In particular, it established regulations for personally identifiable information and deemed the misuse of this data, or insufficient care during handling, to a breach. Breaches under this regulation can lead to large fines for the companies involved.

The basic idea of this standard is that merchants and organizations that handle cardholder data must implement certain technical and organizational measures to ensure the safety and further proper handling of this data. Those rules address the storage of cardholder data, its use for verification or payment authorization, two-party and three-party payment schemes, and its transmission over the internet. Scope data defines the types of data for which regulations must be adhered to. The volume type refers to the data types stored at more than one service provider, while the flow type refers to the data types where cardholder data flow through one provider or more. The summary of flow types and location mapping directly requires further specific security measures to be implemented. Packet traces are needed to create the flow type mapping, and it can be used to verify the effective implementation of the flow type requirements. Cardholder data is split into three types: The card number itself, referred to as the Primary Account Number, the card expiration date, and the Card Verification Value. However, so-called masking can be used to lower the impact of a data breach, even for masked data types. Therefore, the scope of sensible card solutions is not only the type of data but also its geographical flow over service providers.

6.9.1. PCI DSS Requirements

The Payment Card Industry Data Security Standard (PCI DSS) was established to protect consumer payment card information, reduce the likelihood of payment card fraud, and prevent unauthorized transactions. The PCI DSS is applicable to all entities that store, process, or transmit cardholder data, or that control access to these systems and environments. Failure to comply with the PCI DSS may result in loss of merchant processing privileges or fines imposed by a merchant processing bank or payment card organization. The PCI DSS is the requirement of the Payment Card Security Standards Council. The PCI SSC publishes technical documents to assist merchants and service suppliers with PCI DSS implementation.

The PCI DSS, first published in December 2004, was created as a joint effort by major credit card organizations as a unified set of card payment industry security standards. Version 4.0 of PCI DSS was released in March 2022. New objectives require stakeholders to understand information security requirements as they relate to the PCI DSS standards. PCI compliance is mandated for any business or organization that accepts credit card payments through physical or virtual point-of-sale terminals, in-store, over the phone, by email, or other channels.

The PCI DSS contains the following twelve high-level requirements for achieving and maintaining a secure payment environment: build and maintain a secure network and systems, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. Each major requirement has specific and measurable sub-requirements associated with it. The PCI DSS recognizes that it is not always practical to implement a specific requirement. Additional documentation is provided by the PCI SSC for assessing the PCI DSS scale of implementation for Level 1, Level 2 to Level 4, and service providers.

6.9.2. GDPR Implications

GDPR regulations relate to both the Payment Gateway and the merchant. Payment Gateways are often labeled "data processors" under GDPR classification. Data processors do not have full responsibilities and implications in regards to GDPR as data controllers have, but fulfilling processors' obligations must be regulated under a Data Processing Agreement typically necessary when the Data Controller provides confidential information and personal information of customers to the Data Processor. Additionally, the Data Processor must offer extensive security regarding the Data Controller's customers' data protection, as in the case of keeping this data secretly and adopting technical and organizational measures to ensure that unauthorized access to this data is impossible. In case of a data breach, the Data Processor must report it to the Data Controller without any delay.

Payment Gateways are obliged to comply with GDPR if the merchant who uses their services is located in the European Union or offers services to users from the European Union. In such cases, the merchants and the Payment Gateway share joint responsibility over their customers' personal data. GDPR describes the Payment Gateway as a Data Processor. Payment processes are also excluded from GDPR provisions.

The merchant is GDPR-compliant if it meets specifications regarding the processing of personal data. The merchant pays cyber insurance to cover GDPR fines if a data breach occurs, and the merchant is found not to fulfill GDPR compliance rules. The merchant must provide its name, address, contact information, and contacts regarding data processing topics such as training and educating employees in data processing and protection, as well as cooperation with authorities in case of a data breach. Affected data subjects' complaints may also be accepted through these contacts if a merchant disregards its obligations.

6.10. Incident Response and Management

Unfortunately, even the best defenses can be bypassed and incidents can occur. For organizations using payment gateways or processing networks, an incident can mean the leakage of thousands, or even millions of users' credit card information. Organizations can therefore benefit from a well-defined, efficient response and management framework to mitigate harm. When an incident occurs, upon being notified, either externally or by internal resources, IT security and incident response officers investigate the incident's electrical signature for scope and source of the problem, taking into account various detection and alerting methods. The validation of the events leading to the incident are then reconstructed and organized according to a timeline, based on available logs from different sources. Communication about the incident is then established, along with the preliminary assessment about potential impact. A strategy for containment, eradication, and recovery is then formulated and implemented, while avoiding secondary access paths. In the subsequent phases of incident logging and documentation that preserve evidence for possible future prosecution of affiliates of threat actors, less critical systems can be gradually brought back online, while services already restored with appropriate sanitization are being monitored for possible backdoor access.

Once the actual incident is managed and remedial action is taken, the organization needs to identify and document lessons learned, assess the effectiveness of its incident response plan and crisis communication strategy, and be mindful of any legal implications. It needs to refine its response plan so that it is better prepared in dealing with similar events in the future. Preparation is vital; indeed, an organization unable to learn the lessons from its response efforts and put them into action may pay a heavy price at a future date for its mistakes. As such, being smart about the security of payment gateways and transaction networks is as much about learning from experience as it is about technical expertise.

Fig 2 : Incident Response & Management Lifegraphics

6.10.1. Developing an Incident Response Plan

All businesses that deal with electronic commerce and transactions should establish an incident response plan. It should be maintained in a documented shape and revised based on the sensitivity of the data processed by the entity and any surrounding risk factors that would correspond in any modifications to that plan. An incident response plan should be converted into a formal incident response procedure and dated as it is approved. Such document should be stored in a safe place for future review or updates.

Preparing in advance for an incident will alleviate chances of large losses if an incident does occur. It's important that every employee assents to the incident response plan, even if it just means reading and becoming aware of its contents. Incidents typically occur on weekends, holidays or in the middle of the night – times when not everyone may be present. To avoid missteps during these stress-filled times, company-wide drills may be conducted to help employees prepare for any incident. Drills are often scheduled, but "mock" incidents are also created without forewarning to test an employee's response time. Feedback after such incidents can reinforce and refine the effectiveness of the response team and the incident response system.

At a minimum, the incident response plan should include an introduction, explanation of incident response team duties and membership, and incident classification and incident reporting. When an employee suspects an incident, they should know who to notify, even in their absence. The broad classifications of incidents are: breaches in confidentiality, breaches in integrity and breaches in availability services.

6.10.2. Post-Incident Analysis

Conducting an analysis of a security incident after it has occurred is a time-honored approach to improving security. Additionally, conducting a well-done postmortem can help to recover some of the loss sustained during the incident by improving both the company's internal processes and technology, as well as the external products installed at the company's headquarters. However, due to the desire for retribution against both the systems and the users involved in an incident, it can be very difficult to gather accurate and thorough information after an incident has occurred. It is important to make a company policy on post-incident analysis before an incident occurs so that it is clear to all parties involved what will occur after an incident has happened. All team members who could potentially become involved in an incident response should agree to these policies during the preparation of those documents.

When an incident occurs, the policies may then be modified in the context of the incident, but revising incident analysis policies on an ad hoc basis during an incident can hurt the effectiveness of such analysis. Additionally, as an incident progresses, wrapping up that analysis with discretion and sensitivity to the parties involved is critical; policies governing the postmortem procedures should also require that discretion and sensitivity. Once again, revision of these policies before an incident occurs can help prevent conflicting desires to gather information quickly to effect rapid recovery from the company's ongoing security needs. Lastly, it's important to remember that the incident has already occurred; focusing too heavily on program failures and mistakes made by people during the incident can lead to incomplete and inaccurate data gathering, and bitter resentment from the personnel forced to carry out the assigned tasks.

6.11. Future Trends in Payment Security

Payment security is on the verge of radical, disruptive change. There have been many or even innumerable technologies that were created from the 1950s onward that were centered on securing the banking transaction network: tokenization, encryption, biometric identification and verification, artificial intelligence, risk analytics, private and public blockchains, distributed ledger technology, digital currency, the omnichannel world of transactional purchase devices. However, none of these technologies has changed the security payment network. In large part, this is because each of those individual technologies has been added on top of a restrictive legacy architecture. This is also a sign of the resistance of the legacy network to change. The industry risks falling into the trap of asking the annoying question, “What is the future?” instead of asking the important question "What if?' Why is searching for potential disruptive technologies more important than predicting specific evolutions? As taught, “The test of a first-rate intelligence is the ability to hold two opposed ideas in mind at the same time and still retain the ability to function.”

Blockchain Technology

Blockchain is an exciting technology that has a great potential for being a possible disruptive evolution, because it combines many of the easier potentials, and because of the unpredictable consequences of the combination. Blockchain offers the promise of a disintermediated but secure transaction. It uses a distributed network of nodes to store a remote transaction log, but more importantly, ties transactions together in a string, creating an irreversible contract between all of the partners in a business chain. Blockchain also has the security advantage of using multiple cryptography and key systems to use both standards at the level of business but also ample room for privileges with user recognition to meet legal rules and special security needs. The promise of blockchain technology is revolutionary, for the financial and transactional business networks. It offers the possibility of making smoother and more user-friendly transactions while at the same time increasing security by eliminating redundant databases and digital processing nodes. It also provides the potential of making organizations transparent, while making users empowered.

6.11.1. Blockchain Technology

The deployment of payment gateways has revolutionized online transactions, as e-commerce has become a major source of income for many businesses. The Payment Processors have facilitated cautious money transactions without the requirement for paper checks and reached international customers without needing a physical address. As business transactions are moving online, so is fraud; hackers have started exploiting loopholes in Payment Gateway API or network architecture. Payment Gateway service companies provide the security for the transaction process and are responsible for the operations and security of stored data, which include sensitive customer and credit card information redeemable by forging online purchases. After successful completion of the transaction detection, the money is transferred from the customer to the seller without the involvement of any physical or third-party transaction; however, a significant percentage of digital frauds can be avoided if the merchant collaborates with the Payment Processor. In future transactions, customers may have the option to complete payment without the need for a credit card but instead use their phone functionality or e-mail, providing further privacy. Independent payment services have the capability to intrude to the merchant's bank; however, the fees levied on these extra facilities by these independent resources is still an issue.

Blockchain Technology can address security concerns since the individual blocks are safely chained together, thus safeguarding digital currencies. In a blockchain system, all customer payment transactions associated with a merchant will be registered in the linked blocks. The ledger design employed ensures complete transparency and ensures that a tamper of an individual transaction becomes well evident. Although the entire transaction process is well documented for verification purposes, the data are anonymized such that the purchase history cannot be traced back to the individual customer. Another successful deployment of managing wallets would be to utilize entropy or utilize customer's device ID to generate wallets that are activity based for a specific merchant. Only wallets that are actively associated with a merchant will have an impact on the other wallets preventing ripple effects on random wallets. The discussed design is less prone to compromise due to the operating source constraints associated with detecting random wallets that may be observe stealing.

6.11.2. Artificial Intelligence in Security

From the development of solving equations, to automatic theorem proving, to applications of AI in solving specific tasks has a long history. However, industries tended to view AI as a set of specialized programs that can solve narrow tasks, not as a general purpose technology that would revolutionize the development and use of all technologies. The release of made industry rethink their views on AI. engages in sensible dialogues with users, it can generate essays, poems, or program code that are often indistinguishable from that written by humans, as well as correct answers to a variety of queries rightly or wrongly said to be beyond the scopes of prior AI. Prompted by the initial successes of researchers develop and release numerous specialized packages.

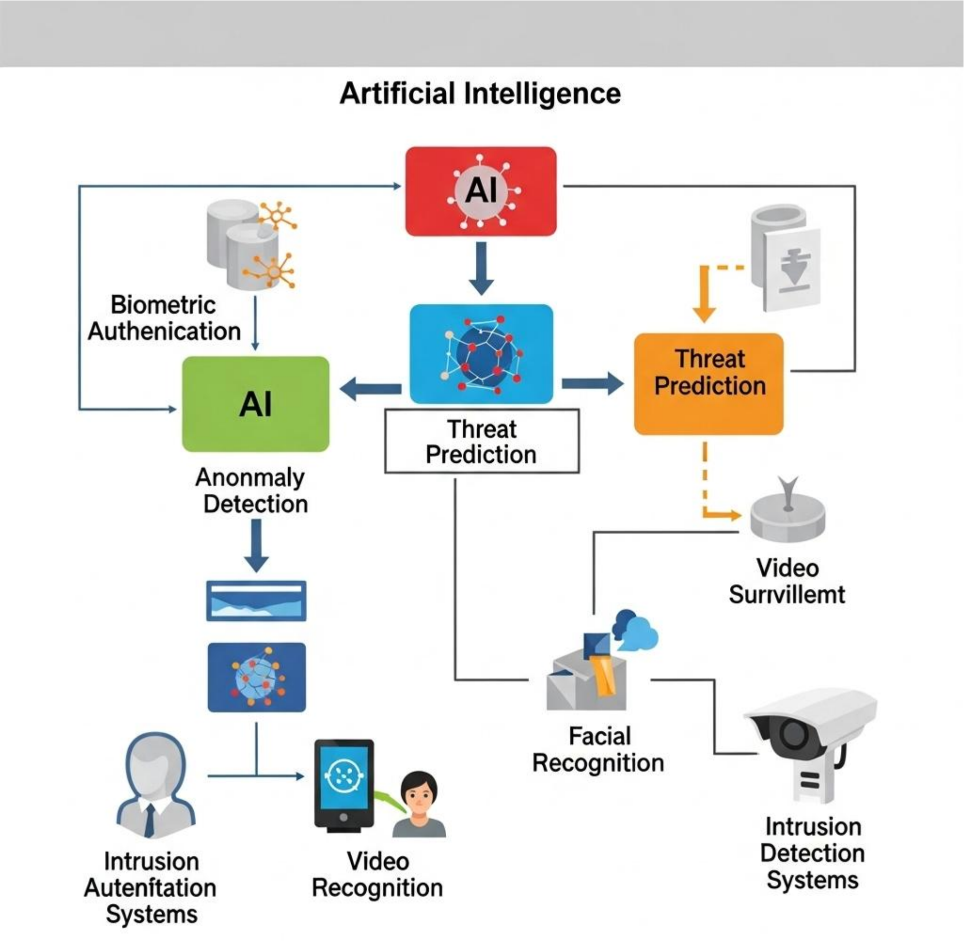

Fig 3 : Artificial Intelligence in Security: A Comprehensive Overview

For security, in the short term, Prompt engineering for AI will be the next big thing. In parallel to AI utilization for security technology development will take off. Vulnerability discovering will be much more efficient, because AI will be able to infer and derive all possible directions of code execution and generate the equivalent risky input for each direction as a human expert. AI will increase the performance of all phases of Intrusion Detection and Intrusion Prevention System, by making intelligent guesses of settings and learning rules for. AI will enhance Phishing detection and Deceptive Click-Through Rate Prediction, by learning from the enormous collection of images, emails, and. Further in the years to come, newer and advanced applications will go beyond the current use of AI for security. Security engineers will start to make intelligent guesses on what attacks will come based on the larger context of the organization, embed better counters in the system, and predict counter-counter attacks to ensure better defense.

6.12. Case Studies of Payment Security Breaches

It is always better to learn from someone else's mistakes. That is why breaches of other payment gateways are analyzed. A selected list of breaches is identified. The reason for their breach is also detected by establishing chain of events that constructed the vulnerability, leading to a security breach. After that, possible defense mechanisms are proposed to prevent these similar attacks.

Before the attacks in this chapter are analyzed, it is pertinent to give some numbers on breaches. The number of websites infected with malware designed specifically to steal online banking information rose significantly, reaching a high number of sites in the fourth quarter of a recent year. Phishing is estimated to be much more likely targeted at financial services than any other industry.

Many of the recent intrusions into retailers occurred when hackers used malware to steal POS transaction data that contained payment card information. A large number of stores were breached, targeted by hackers who successfully injected malware into the retailers' networks that caused customers' payment card data to be stolen when the card was read by the POS terminal. Investigations revealed that, following the installation of the malware, none of the retailers had implemented certain security measures that were required by industry standards. Specifically, they failed to utilize proper segmentation, thus allowing the hackers network access to the unprotected payment card data.

The only way payment gateways are going to have success combating fraud online is recognizing that we're all in this together. As opposed to looking at it as an adversarial position — the bank doesn't want to approve the transaction because they want to save money and the merchant doesn't want to pay for chargebacks — if we can get together, we can use our combined intelligence to validate transactions better, pointing towards one direction and creating something that people want to use, not something that's overly burdensome.

6.12.1. Analysis of Major Breaches

Sections 1.2 through 1.8 provided examples of some of the most significant security breaches that specifically affected payment gateways or transaction networks. The content was drawn predominately from media reports and provided in the necessary detail to cover the significant issues involved in the actions. In this section we will make extractions of key information gathered to apply our knowledge and create an analysis of those actions. The breaches mostly forgone cover malwares and DDoS attacks. The specific focus on criminal acts that specifically relate to payment gateways, transaction networks, and the financial industry is what positions this content more in the area of payment security than general network or application security.

There are several reasons why these attacks should be discussed at length. From a technical standpoint, the payment industry's technological problems mirror general IT issues highlighted in industry-wide reports but in a more specific manner. Secondly, people expect banks to be bulletproof. We focus on the major players to demonstrate that they are infallible. Security issues in technology have all but disappeared in the banking industry. There are bank offices on street corners and almost no ATM or teller theft anymore. Identity theft has become a key focus for law enforcement and payment security experts. It is in the area of e-commerce payments that the major security flaws now exist. In other words, the payment industry has seen major increases in well-publicized, costly data breaches but not a corresponding increase in failed payment transactions. Detection, prevention, and insurance against fraud are paying off.

6.12.2. Lessons Learned

Different payment security breaches, most of which might not be publicized for some reasons, can have different scopes. However, if we list the payment security breaches in no particular order, we might conclude that they have some points in common which might help us understand how we could avoid facing these different kinds of breaches. This section explains the lessons learned from significant payment security breaches.

Lesson 1: Payment Security Breaches Harmed Tens of Stores and Thousands of Customers

Security breaches for the payment gateways hosting the virtual stores can affect physically none of their stores, since those are not hosting servers for them. However, a data breach in the central payment gateway can harm thousands of stores, customers and/or banks. Security breaches are harmful for the store where the transaction occurred and also for the payment provider. When transactions are processed and stored for review later, reports have to be prepared in order to know what the harmed customers suffered and possibly recover them of the damages they have faced.

Lesson 2: All Kinds of Data Can Be Exposed in Different Breaches

Different payment breaches can expose different sensitive data, depending on the way they are monitored and the process that has been put in place to deal with them. Moreover, some data have more value for hackers than others, as long as different strategies can be used to harm the victims. For instance, credit card number, expiration date and card verification number can be used in criminal activity since stolen credit cards can be used in a large range of transactions. Data leakage with authentication credentials can also lead to a high number of breached accounts allowing the attacker to fraud the people whose account has been taken.

6.13. Best Practices for Securing Payment Gateways

Although payment gateways are necessary in e-commerce operations, they may lead to several security issues. Threats such as man-in-the-middle attacks may violate the confidentiality and integrity of payment transactions. In addition, transaction information may be compromised by malware on the merchant-side. Therefore, implementers should pay attention to the design and integration of payment gateways into merchant systems, and security controls should be integrated into their features so that parties are afforded a low-risk environment.

Consent management allows a merchant to get necessary permission from a user, such as executing a transaction, even in cases where the amount or transaction type was not explicitly stated as part of the user agreement. Users must be aware of the purpose of the gateway, and merchants should give clear information concerning what data is being collected and why it is being shared with the gateways. Legitimate gateway user interfaces should have a well-designed look and feel. Payment portlets need to be carefully designed such that it is clear to the user that they are indeed entering the payment data to the gateway and not just doing it in the merchant's webpage.

Furthermore, portals and other functionalities need to be provided by the merchant, but the security focus is on data transmission handling. The gateway should use encryption algorithms that provide required levels of confidentiality. Communicating through TLS is often the simplest and fastest way to secure payment transaction networks. Secure codes should be used to conceal credit card numbers, CVVs, PINs, checksums, and other sensitive data. Payment gateways need to implement security measures for privacy protection, such as data masking.

6.14. Conclusion

It is impossible to ensure that a transaction is performed by a legitimate user of the payment method. However, by approximating these conditions as much as possible, the risk of losing money with a transaction can be diminished. We have detailed the best practices to follow when securing payment gateways and transaction networks. These practices target different aspects of a transaction, from the methods used by its issuer to analyze it, to the experience and reputation of the merchants that receive it. Recently, the incentives in the ecosystem that offers card payment methods have taken payment brands to make some risky decisions that increase the risks excluded in this document. For instance, the common validation process of merchants was axed, in which they were segmented on the basis of the volume of transactions they processed. With this, some small merchants now go years without commercial requirements and evaluation. Other merchants falsify their Database Validation Merchant history to avoid being fined. The same happens with the banning of account verification before any deposit type. Other excessive customs refer to the prohibition of charging the transaction on behalf of the merchant that is responsible for it.

As we have shown, the best observable method available to avoid transactions being performed by fictitious and undeterred users is to analyze the entire transaction lifecycle. How the deposit was executed, how it is then transmitted to a third-party company, how that company delivers the product or service, how the payment is settled, and how the address details are for both the issuer and the receiver are a few of the numerous steps through which a transaction goes. If some precautions are taken and some methods are followed when doing this, then the risk of being a victim of fraud can be reduced to reasonable levels.

References

S. S. M. Chowdhury et al., "Securing Payment Transactions: A Comprehensive Review of Smart Cards and Contactless Payments with Cryptographic Methods," *IEEE Access*, vol. 13, pp. 10234–10250, 2025.

M. A. Hossain et al., "AI-Enhanced Fraud Detection in Real-Time Payment Systems: Leveraging Machine Learning and Anomaly Detection to Secure Digital Transactions," *Australian Journal of Machine Learning Research & Applications*, vol. 2, no. 1, pp. 45–56, Mar. 2025.

K. Yamini et al., "An Intelligent Method for Credit Card Fraud Detection Using Improved CNN and Extreme Learning Machine," in Proc. 8th Int. Conf. Commun. Electron. Syst. (ICCES), Coimbatore, India, pp. 678–683, 2023.

O. Wang, "Explainable AI for Credit Card Fraud Detection: A Review," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 5, pp. 2301–2316, May 2023.

H. L. Liu and H. Li, "Deep Learning for Credit Card Fraud Detection: A Review," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 1, pp. 237–247, Jan.–Mar. 2022.