Quest Journals
Journal of Software Engineering and Simulation
Volume 7 ~ Issue 9 (September 2021) pp: 46-53
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Challenges and Checkpoints of Payment Systems Security

Balaji Soundararajan
Independent Researcher

Abstract
The transition towards a cashless economy has amplified the importance of securing digital payment systems against evolving cyber threats. This study examines the vulnerabilities inherent in traditional and electronic payment systems, including credit cards, mobile payments, and RFID technologies, while addressing emerging risks such as data breaches, fraudulent activities, and network attacks. Through an analysis of case studies and current literature, the paper evaluates the efficacy of security measures like encryption, tokenization, multi-factor authentication (MFA), and compliance frameworks. Findings reveal that while technological advancements offer convenience, they also introduce complex vulnerabilities requiring layered security strategies. The study underscores the necessity of aligning technical safeguards with international standards, fostering stakeholder collaboration, and adopting proactive fraud detection mechanisms. By highlighting successful implementations and lessons from security breaches, this work advocates for adaptive, user-centric approaches to mitigate risks and sustain trust in digital payment ecosystems.

Keywords
Payment systems security, Electronic payments, Fraud prevention, Data breaches, Encryption and tokenization, Multi-factor authentication, Cybersecurity frameworks, PCI DSS compliance.

I. Introduction

Payment systems have different underlying technologies, that introduced various security vulnerabilities which, with the passage of time, have risen as a key focus point. Almost every week, there is a news headline concerning an IT security failure with a vast impact on businesses or the everyday life of consumers. The increasing number of retail payment transactions worldwide and their vulnerability invite thieves and hackers to compromise payment transactions and thereby steal sensitive payment transaction information, which threatens individuals' privacy and causes fraudulent activities. Payment system security is a critical requirement for building trust in the e-commerce industry among consumers and for the wider spread use of e-governance. An insecure retail payment system would impede transactions and pose high frictional costs on the economy. The first point of contact for both consumers and businesses can get compromised due to lax security at various physical and electronic frontiers. These collective vulnerabilities and the presence of fraudsters from various world regions hinder the elimination of fraud, financially speaking. Interestingly, RFID fraud and network attacks have also been shown to threaten the privacy and safety of micro-payment transactions that utilize RFID technology. It is important to mention that this sometimes negatively correlates with socio-economic parameters in various world regions, highlighting a crossroads human conundrum and vulnerability against combating global security threats. Owing to that fact, the increasing impact of vulnerabilities in today's static technology has received significant attention from various related forums. As a result, the warning about 'cyber-physical threatening attacks' that specifically compromise ICT systems supporting payment transactions has underscored the requirement of this work.

Importance of Payment Systems Security

As long as trade exists, there is a need for a payment mechanism. In the old days, cash in the form of coins and banknotes was used when people were purchasing goods or services. With the improvements in information technology, particularly in communication, more effective alternatives have been designed. These alternatives have attracted a considerable market share and are going to replace the classical methods. However, this cannot be conducted without neglecting security.

Although we do not see fraud, we daily hear stories regarding the unauthorized access of bank accounts or the hijacking of credit card details. These risks originate from internet-related risks, and from this perspective, they are assumed to be higher compared to ordinary face-to-face business transactions. If we talk in business

language, transaction integrity and trust are the issues that stem from transaction security. People tend to use payment mechanisms that help establish a safe and secure transaction environment. At the level of government, these issues are also under review. In the EU, there are more than 10 regulations directly related to payment systems and electronic transactions. In addition to this, there are more than ten studies, opinions, guidelines, and papers for payment systems security. Legislation has been created not only to cover the issues related to the commerce of goods and services but also to create trust in the payment mechanism to assure the stability of the economy. High-profile data breaches emphasize the need for an effective approach to security.

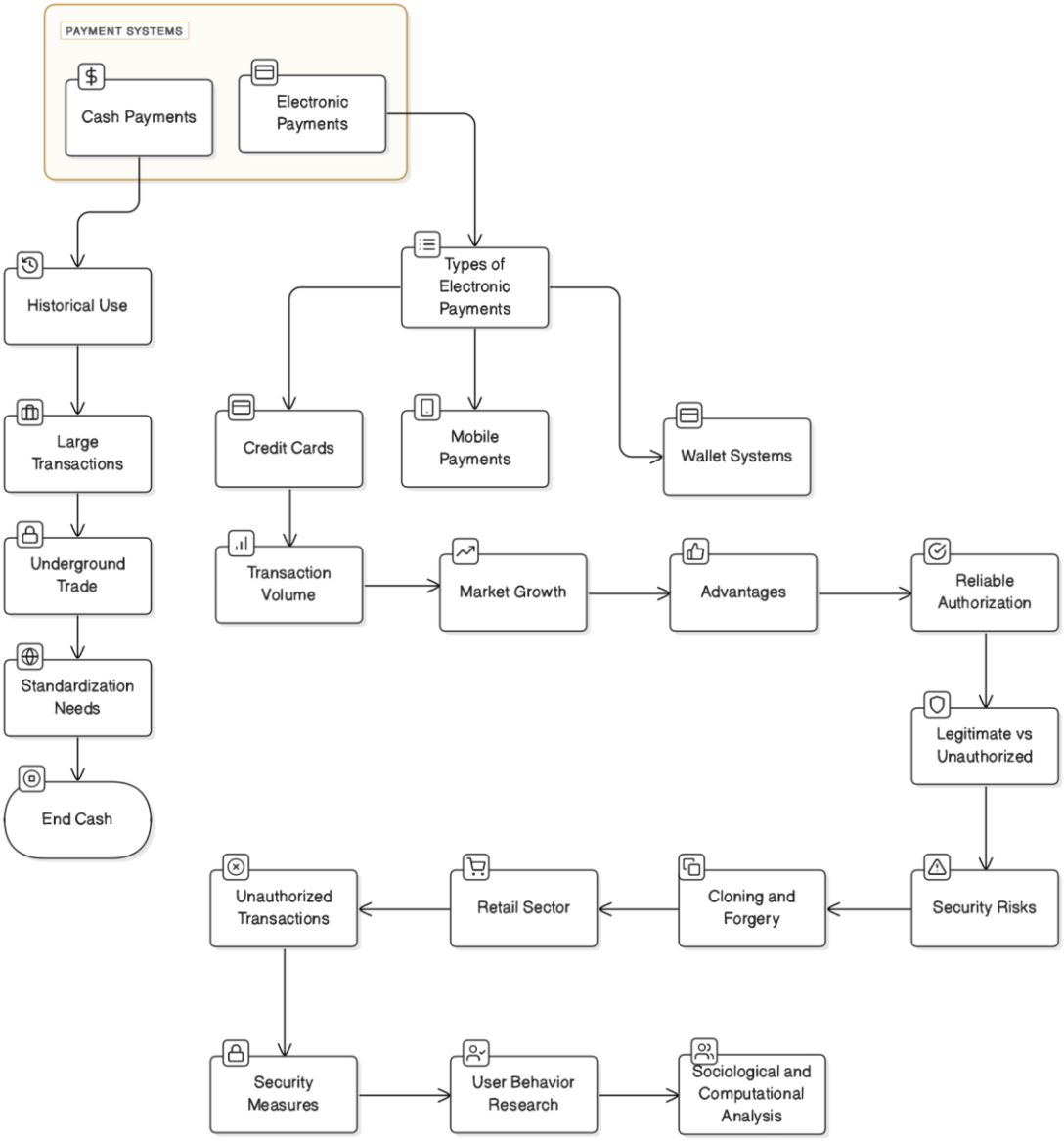
Purpose and Scope of the Study

Payment systems are becoming increasingly important in today's commerce. This work deals with payment systems security. The purpose of this study is to provide an analysis of payment systems security: threats and counteractions. We also review traditional and electronic payment systems and the security problems and challenges of their operation. There exist many questions that need to be addressed in the area of payment systems security: "What are the security threats that require special countermeasures in this field of e-commerce?"

The objectives of our study are the investigation of such important security topics and the assessment of the security gaps of the selected payment methods: traditional and emerging ones. To meet the objectives, the paper presents the following research questions: - What are the new security threats and frauds that have to be taken into account in the field of payment systems? - On the basis of which legal acts and high-level international standards are payment systems safety requirements formed? - Are the current technical and organizational security mechanisms of the selected traditional payment systems efficient enough to minimize the possibility of system impairments, fraud, and forgery? - Are the technical and organizational security mechanisms of the hybrid online payment gateway in line with high-level international standards? - Is the usage of the above-listed technical and organizational safeguards sufficient to provide a complex security solution, including secure money transfers and effective platform protection? - What are the best practices of the security tools and solutions acknowledged by the relevant scientific and professional communities that can be implemented in building next-generation financial systems? - In what ways do years of academic research and commercial large-scale systems deployment associated with the development of a secure and failure-tolerant framework relate to the selected payment systems protection? The study provides an analysis of the current literature and processed case studies. All of the above questions mentioned are also elaborated and answered in the body of the work. The study is organized as follows: an overview of payment systems and the security of payment types is provided first.

Types of Payment Systems

Classifying the most prevalent payment systems provides us with the two categories depicted in the diagram. Cash payments may not be groundbreaking, but their forefather status makes them worth including despite the narrow spectrum. They have been used in some form for centuries and are currently used stage-wise for larger transactions or for underground trade due to their fictitious nature. Their standardization requires an international basis for the definition of large transactions and bulk cash movements to differentiate them from small retail purchases. Examples of traditional electronic payment systems are credit cards, mobile payments, and wallet systems where a user binds their payment data up front or provides it as needed. These are clearly the systems taking most transactions; the latest usage statistics give figures of about 22,000 and 24,000 credit card transactions per minute in the United States, for example. [1]



Market growth of electronic systems also points to a biased nature to our needs. Their advantages include the reliable authorization of payments and the ability for banks to distinguish between legitimate and unauthorized payments. Yet they are also more subject to attack from the technical cloning of credit card information for replay or forgery, typically in the retail sector, where businesses take it upon themselves to authorize or reject transactions. This corresponds to the ease and ubiquity of their use with the potential to conduct unauthorized and/or fraudulent transactions, as distinct security measures for various payment systems can be evaded. Therefore, a complete examination of payments to exploit the user's comparatively greater load on the research seeking to understand user behavior from a sociological and computational stance has been undertaken.

Cash-based Systems

In the era of technology as a solution and obstacle, it is easy to forget that payment systems also include the general acceptance of cash. In a general sense among the list of payment systems most practitioners recognize, it stands alone in several respects. First, cash transactions are anonymous: bank tellers do not need to ask your name. Secondly, control responses to fraud are limited: no financial institution will protest an alleged policy requiring that they refund your cash after it has been stolen from you. Third, offenders associated with cash are likely to be greed-based with theft of the payment rather than the act of purchase, whereas for online purchases the act of purchase itself may be viewed as the object of the theft. Finally, cash is immediate. This set of characteristics for cash seems to cater to a specific kind of customer. However, its anonymity, as noted earlier, poses serious problems with accountability. Systems set up to launder money integrate cash with the

tasks of numerous interchangeable agents of varying size, making it exceedingly difficult to determine where bad acting first takes place.

These reasons make cash transactions vulnerable to theft. Users relying mainly on cash transactions include minority groups in the minority world (those with issues of addiction in particular) and most people in the majority world. Those who are uncomfortable or unequipped to engage in technology transactions will also rely to a greater degree on cash. In some countries, only tourists are asked how they would like to pay for their goods at the point of sale, because they are the only ones without the means of paying digitally. A slew of opportunities pose security risks when money is handed out. Typically, during the day, cashiers fill the till from a safe, and then when the till is full, exceptional procedures are used to get rid of the overage. Managers do so in one of several ways, including skimming and direct multiple cash drawers. They then usually enter a manager code granting them access to the drawers. There are, of course, advantages and risks when it comes to cash transactions.

Electronic Payment Systems

Payments and transactions have substantially transformed the way people get their financial transactions done. Users can now use credit cards, debit cards, go to a local bank to pay their phone bills and utilities through online banking, and alternative cryptocurrencies for their mobile top-up transactions. To date, there are multitudes of electronic payment systems in existence. The most commonly used electronic payment medium is credit/debit cards. This requires an interface with a card reader, as checking the card for a transaction would require a payment order to be transmitted to a bank or a credit agency. The cheapest and well-established electronic system of the bank became their own financial institutions. Customers of the banks were initially capable of seeing their accounts through an ATM or through a telephone but can now pay bills and move money through the usage of their own banks' online banking platform. One of the popular means of shopping online through credit card facilities typically depends only on a personal computer or smartphone with the aid of an online web browser to link users to the retailer's site. Among the latest possibilities is the option to pay by mobile devices. Mobile financial systems provide the convenience and access consumers have in the modern world. A trust system for customer satisfaction is essential between all parties involved. With new technology and software advancements come security risks. These include hacking, information about customers, information about business practices, unlawful importation, card theft, refused payments, and viruses. Over the years, communication within mobile networks has opened the transmission to a multitude of attacks. The main security issues will include changes and modifications, availability, trust, and auditing. Some vulnerabilities have been recently addressed as they require better protection to secure customers and businesses. Whatever the infrastructure, most security barriers such as customer confidence, enforcement, and authentication can be addressed from the point of view of protection. [2]

Security Threats in Payment Systems

The global banking system is an example of a highly integrated and evolved payment system. With advances in digitalization and information and communication technology, there has been a dramatic increase in the sophistication of security threats; the use of new technologies and operational methods absorbs all advances, making cybersecurity a global concern. In Uganda, the situation is not any better. The number of reported cyber incidents has significantly increased in the last three years. The incidents encountered include hacking, unauthorized access to information systems, website intrusion, system failure, identity theft, data breaches, financial fraud, and automated teller machine skimming. Payment systems are one of the most affected information systems. Hackers can use account holders' names, addresses, national identification numbers, social security numbers, usernames, birth dates, email addresses, and bank and credit card account numbers to conduct transactions as if they were real account holders. Threat actors can exploit these vulnerabilities in various payment systems to gain unauthorized access or to replace, delete, or manipulate the content of a legitimate transaction.

The fraudulent transaction could be conducted by using the cardholder's information from a cloned card. As a result, various electronic payment systems maintain specified security methods and mechanisms to protect information assets from unauthorized access. A data breach is an event when an explicitly authorized entity observes, copies, disperses, or uses or tries to use information. From data, merchants lose their credibility with their customers. Payment transaction systems encompass various types of financial schemes that emphasize different phases of the entire payment process. The transfer of money from the remitter's bank account to the beneficiary's account is the result of a coordinated set of systems. The messages exchanged between different entities are used on the basis of secure networking, authentication, and encryption mechanisms, and consumer transactions use remote access and a combination of secure communication protocols. The stakeholders consent that the nature of system risks in the payment industry is influenced by the specific business being conducted

and the regulatory environment in which they operate. Banks, businesses, and the payments industry consider many measures and control mechanisms before allowing customers or merchants to use payment facilities.

Fraudulent Activities

Fraudulent activities systematically affect payment systems. Practically all specifications in payment processing have been attacked over time. Fraudster techniques are sophisticated, beginning with the collection of personal information and the validation of potential victims. Traditional credit card fraud also occurs when goods are purchased with stolen valid credit card numbers. Customers may also fall victim to phishing and other email scams. Phishing is the art of defrauding an online account holder of personal information by posing as a reputable company, typically an online bank or merchant. Once the fraudster has this information, the stolen credentials of the real account holder can be used to validate newly created fake accounts. The consumer's frustration of having to prove they are not guilty in such a case affects consumer trust and a retailer's willingness to do business online. The rise in the last 10 years of asset and identity theft has given new opportunities to criminal cyber activity. The technological advance has made fraud attractive for individuals. It is expected that cybercriminal behavior will rise in the future. Cybercriminals are usually fake website designers and typically operate in international jurisdictions that are difficult to police. Law enforcement agencies, and by extension society, have difficulties apprehending them. New methods for fraud prevention must detect the adaptable cybercriminal. Fraud detection systems use various tools ranging from knowledge-driven rules to technologies that perform intelligent data analysis. Machine learning algorithms and behavioral analytics are now used globally in the finance sector to detect and prevent fraud. [3]

Data Breaches

Data Breaches In the current state of the payment systems industry, the possibility of a data breach looms large. A data breach can involve sensitive information, such as consumers' first and last names, email addresses, and password reminders, as well as personal user data like billing and shipping addresses. It is no overstatement to say that data leaks, breaches, and hacks have become everyday risks in today's connected world. The majority of external hackers use technology to initiate a breach. Inadequate organizational staff and business partners are the culprits in the remainder of cases. This paints a picture of attacks in the form of hacking, financial harm, and insider sabotage. The end of a data breach is not the end of the story; the aftermath can deeply affect both individuals and organizations. Organizations lose money, consumers become disenchanted, and businesses face fines and legal punishment due to lasting reputation damage and future earnings loss, among others.

Having a final and detectable program in place can mitigate the impact of a data breach. The damage from a data breach can be expedited, and organizations can be held responsible if the affected party loses money. Organizations have a variety of solutions to select from, and there are several laws and regulations in place in the payments industry to improve accountability. Following a breach, organizations and payment card-issuing banks may be required to reimburse consumers who suffer financial losses. The extensive debts, disruptions, disputes, and threats to PCI DSS are continually evolving. As a result, organizations must be proactive in their development of security initiatives. Tokens, verification, transaction and fraud monitoring, next-generation matching, and security strategies are examples of security strategies that are becoming increasingly popular. As businesses and customers embrace new technologies, they also need to adapt to today's electronic payments industry. Cybersecurity solutions, including fraud detection and prevention, continue to evolve to keep up with changing technology.

Security Measures and Best Practices

As the threats and attack vectors evolve and change, so do the security measures. Over time, a number of security measures and best practices have been identified and documented. These can be clumped into two primary classes: technology and partnerships, and staff and physical security. Technology measures include antivirus, firewalls, software updates, hardware updates, and training. This 'layered security' provides different technologies and different protocols with which different technologies are implemented.

Policies are disclosure and dispute mitigation measures. They provide mechanical security—security by requiring that systems be safe before they interact with the network. They don't directly stop attacks, of course, but should strong security controls fail, they provide additional lines of defense. Some up-to-date recommendations for establishing secure environments are provided. Some of the steps toward enhancing the security of a payment system are as follows: (i) Review and update security measures. At least once a year, security should be reviewed. Any new developments or technological advancements that might call into question the efficacy of existing security should be addressed. (ii) Train your staff. A secure technical infrastructure is a necessary but not a sufficient condition for payment systems security. Well-meaning clerical mistakes—errors in processing, system configuration, or storage of payment card data—can compromise a

system as effectively as the most cunning hacker. (iii) Have an Incident Response Procedure (IRP). Every business suffers a data breach. Choose how they happen, or when they happen, and choose to train your staff on your IRP or respond on the fly. [4][5]

Encryption and Tokenization

Encryption is the process of encoding plain text into unintelligible text to prevent unauthorized access to the content. This ensures data confidentiality and, when supplemented with other measures to protect data in transit and data at rest, encryption is an essential technology in payment systems security. A variety of encryption techniques exist, including algorithms, key sizes, and methods for the exchange of public and private keys, and trigger processing that includes symmetric encryption, asymmetric encryption, and hashing and public key. The most common encryption methods used in payment systems include Secure Socket Layer, Secure Electronic Transaction, and the more current, more secure alternative, Transport Layer Security, the use of each dependent on the specific system and service architecture. The practical use of encryption to secure payments would apply, for example, to the digital wallet services using tokenized digital cards to be used with near-field communication technology, or when native or in-app digital tokens are being processed by the smartphone via QR codes in e-commerce transactions or instant funds transfer services. Tokenization goes a step further than encryption in payment applications. Instead of simply preventing unauthorized use of real sensitive data by keeping it secret and jumbling up the original plain text, the technology uses token types, applied at initiation, that can no longer be associated with the original clear text, in-stream payment credential.

Implement the secure Remote Commerce framework that is intended to make online shopping more secure and to facilitate payments across Internet-connected devices, regardless of payment type or 'mode of commerce' where both use tokenization at rest, but only one uses encryption in flight for the interchange payment flow in their 'near true real-time' payment scenarios, i.e., when using HCE. Apart from data security, the tokenization method also reduces the need to store real PAN, CVV, and expiration date details, keys that would, if compromised, lead to personal data loss, can be tokenized/transformed, and stored safely on a network. Organizations must ensure that customer payment data is securely stored, handled, and transmitted in accordance with the relevant regional legislation. In addition, organizations must be able to implement such technologies, for example, by deploying encryption technologies to store cardholder data securely and then applying tokenization and further encryption to support and protect cardholder data added and stored within the systems or to store the tokenized cardholder data of users.

Multi-factor Authentication

Multi-factor authentication (MFA) improves transactional security by requiring the use of multiple verification methods, such as something the user knows, something the user has, or some aspect unique to the user. A common MFA is the use of one-time passwords (OTPs). Most authentication techniques that implement MFA are app-based or SMS-based. Other mechanisms, like biometric data, can help to detect potential fraud; hence, MFA is used as a process of credential vetting.

Challenges around MFA integration include the difficulty of system upgrades, especially in legacy systems where changes required to process an upgrade are both expensive and time-consuming; user resistance to the addition of a new security layer; compliance with existing privacy laws and policies are key; and further, increasingly privacy-respecting architecture, especially as biometric methods become more prevalent due to overall ease of use and resistance to fraud. Techniques for improving MFA acceptance are presented for the healthcare network, as understanding the potential for MFA to enhance patient privacy and security is expected to increase user acceptance. MFA acceptance strategies for military data networks and financial websites have also been examined. Mobile phones featuring biometric identities have been proposed as a possible user acceptance model. Findings suggest that understanding and addressing user resistance and costs are critical to the success of MFA implementations.

Case Studies

In an effort to illustrate the application of the Security Trilemma framework, two case studies were investigated: Zuri in South Africa and the recent Colonial Pipeline attack in America.

Case Study 1: Lessons Learned from Payment Security Breaches - The Colonial Pipeline attack and the case of unauthorized activity on the Zuri system of Discovery Bank in South Africa are recent examples of security incidents. These incidents were selected for the retrospective case study because they represent security failings in different contexts and how these were successfully or unsuccessfully exploited. The Colonial Pipeline attack occurred in the energy industry, while the latent attack on the Zuri system offers details of an attempted, yet unsuccessful, attack on financial services payment systems.

Case Study 2: A Tactical Security Implementation Showcasing Strength in Approaches For the comparative case study, security implementations were chosen from the financial services and hospitality

industries, respectively. The Qhubeke banking solutions ATM monitoring system offers an innovative anti-fraud approach, while the Mozambik Restaurant in Ballito, South Africa, showcased an access control mechanism to its secured area for patrons only. Each of the security implementations of the case studies was chosen in accordance with convenience and availability in the field. This implies that both implementations are situated in South Africa. The advantage of employing this methodology is that the security practices demonstrated provided 'real-world' examples in the form of good and poor security practices, which afford general insights and can be more easily related to existing industry concerns.

Recent Payment Systems Security Incidents

It is of particular relevance to take into account that there have been an overwhelming amount of security incidents surrounding payment systems during the last few years. These have widely been covered in the news one way or another and are sure to be remembered by everyone who has been a victim or suffered any data theft. Some of these payment-related security incidents don't fit within the typical type of payment systems available, yet still deserve mention due to their importance and the fact that the same system principles or other sensitive financial services were affected. Due to this long list, the events hand-selected for the case studies are those that focus on the impact they had on the organizations themselves, the damage and subsequent costs, the impact on their customers and stakeholders, and finally, the system changes made as a result. Data thefts fresh from the oven are of particular interest, and although they may not be fully explored here due to the recency of events making enough analysis data sparse, they do help highlight what causes and impacts such fraudulent activities have. New case studies and events will emerge directly from the data we have collated covering foiled or successful frauds from illegal card usage, stolen card details, or other techniques where organizational assets have been obtained by fraudulent means. [6]

The methodologies used by criminals to gain access to sensitive data have changed. Criminals are now engaging in newer tactics that are more difficult to detect than the tactics of old, often gaining access through social engineering rather than through a direct technological breach. Additionally, this newer brand of criminal is also more specific than their predecessors and has the capability to spend months within a system mining for information. The result is a new, more dangerous, and very costly criminal, capable of accruing damages into the millions. Unfortunately, as the threat landscape continues to expand and evolve, the payment industry struggles to stay ahead. Regulatory bodies have addressed the issue here, changing their policy to mandate compliance to ensure future immunity from multifaceted possible events of a similar nature. Although the threat landscape is too large for organizations to cover all angles, it is important for these organizations to be cognizant of the threats and risks that come with using their payment system. By ensuring steps are taken towards appeasing these threats through the implementation of more stringent precautions, security can be heightened, and for the most part, effective fraud prevention methods can be used to benefit the available system.

Successful Security Implementations

A variety of options and best practices were showcased during the research, offering a glimpse at what has worked for organizations in different sectors. True value in payment systems security shines through the collaboration between service and solution providers and the businesses utilizing them, with these organizations unifying in pursuit of a common goal: enhanced security and an excellent customer experience.

Innovations in Proving / Replacing: A partnership transformed how it verifies payment method users and replaces lost or expired cards. The new approach entailed tokenization for user verification, which is wallet-driven to realize and recognize the cardholder anew when a device token no longer matches an issued token and thus can't be called via messages. A solution was showcased to detail the sophistication in leadership in fraud detection and prevention, malware remote access tools, and behavioral biometrics, providing truly comprehensive security solutions.

Identity Authentication Improvements: A partnership created a virtual coin purse and repriced its contents for a payday and licensed cash lender. The new app improves the company's privacy, reduces internal cybersecurity breach vulnerabilities, limits fraudster access and egress, and lets agents focus on customer relationships instead of private investigations of the user.

Increased Security Can Pay Off for All: There are also some best practices in providing consumers and businesses enhanced security that were discussed, which may not be the right move for everyone. A person-to-person payment solutions platform brought prospects increased security, thus facilitating conversations about the "why" of a consumer-to-business P2P solution. Although it demonstrated unshakable data security, it did not pursue certification, reasoning that it lacked hard data to back up a ROI pitch for this significant investment ongoing security backup program. The company's certification for its information security and infrastructure architecture secured inside and behind the firewall did help sales representatives in their strategic security conversations on occasion.

These certifications are worth the effort for the right organization because they build customer trust, and found tremendous success there. For example, it closed its initial sales push with 356%, instead of the expected 200%, of its benchmark annual sales increase. A case study noted that the certification defrayed up to 5% of a policy premium. A use case for when certification standards saved both internal staff and outsourced infrastructure suppliers 10% of certification costs. Unfortunately, organizations do not pursue certifications for a number of reasons, including staff training failures rooted in shrugging off the need to know what exact steps they need to take. Traditional sales teams do not ask the right questions to companies about certification in the sales process either.

II. Conclusion:

The security of payment systems is paramount in sustaining global economic stability and consumer trust amid the rapid digitization of financial transactions. This study identified critical threats, including phishing, card cloning, and sophisticated cyberattacks, which exploit gaps in both traditional and electronic payment infrastructures. Effective countermeasures such as encryption, tokenization, and MFA emerged as vital tools to safeguard sensitive data, while case studies like the Colonial Pipeline breach emphasized the consequences of inadequate security protocols. Successful implementations, such as tokenized verification systems and behavioral analytics, demonstrate the value of integrating advanced technologies with regulatory compliance (e.g., PCI DSS). To combat evolving threats, organizations must prioritize continuous security audits, staff training, and collaboration across industries. Future efforts should balance innovation with resilience, ensuring that security frameworks adapt to emerging risks without compromising user experience. By adopting best practices and learning from past incidents, stakeholders can build robust payment ecosystems capable of mitigating fraud and fostering long-term consumer confidence.

References:

[1]. PCI Security Standards Council. (2016). PCI DSS (Payment Card Industry Data Security Standard) v3.2. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf
[2]. I. Suwanragsa, P. Sinliamthong, P. Srivalosakul, "Electronic payment system: Types, trends, and its impacts on Thai economy," Journal of Social, 2020. nrct.go.th
[3]. Gupta, S., & Kim, H. (2018). Machine Learning for Fraud Detection in Electronic Payment Systems. Proceedings of the IEEE Conference on E-Commerce, 234–241 ieee.org
[4]. F. A. Khan, M. Asif, A. Ahmad, M. Alharbi, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," Sustainable Cities and …, 2020. [HTML]
[5]. Roberts, M., & Almeida, V. (2016). Data Breach Management: Lessons from the Healthcare and Financial Sectors. Computers & Security, 59, 156–174. https://doi.org
[6]. Nguyen, L., & Wilson, D. (2015). Case Studies in Payment System Vulnerabilities: From RFID to Mobile Fraud. Journal of Cybersecurity Research, 10(1), 22–39. https://doi.org