Volume-04 Issue 10, October-2020 ISSN: 2456-9348
Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

THE EVOLUTION OF CARD PAYMENT TECHNOLOGY: HOW SECURITY RISK DRIVES INNOVATION IN FINANCIAL SERVICES

Oluwatofunmi Ibukun Akinluyi[1*], Tina Charles Mbakwe-Obi[2], and Efemena Connor[3]
[1] Flutterwave Inc. Nigeria
[2]Geo Partial Application Center (GEOAPPSPLUS)- National Space Research and Development Agency, Nigeria.
[3]Center for Satellite Technology Development - National Space Research and Development Agency

ABSTRACT

The evolution of card payment technology has revolutionized financial services, enabling seamless, secure, and efficient transactions. From the early days of magnetic stripe cards to the introduction of EMV chip technology, the industry has continuously innovated to enhance security and protect against fraud. With the rise of digital transactions, new threats have emerged, driving advancements in encryption, tokenization, and biometric authentication to safeguard consumer data. Security concerns have played a pivotal role in shaping card payment technologies. The transition from static card data to dynamic authentication methods, such as contactless payments and cryptographic protocols, has significantly reduced vulnerabilities to fraud and identity theft. Furthermore, regulatory frameworks such as the Payment Card Industry Data Security Standard (PCI DSS) and Strong Customer Authentication (SCA) have enforced stricter compliance requirements, compelling financial institutions and merchants to adopt robust security measures. Artificial intelligence (AI) and machine learning (ML) are now integral to fraud detection and prevention, analyzing vast transaction datasets to identify anomalies and mitigate risks in real-time. Additionally, the emergence of blockchain technology and decentralized finance (DeFi) presents new opportunities for secure and transparent payment processing. This paper explores the technological milestones in card payments, the role of security in driving innovation, and future trends in financial transaction security. As cyber threats evolve, ongoing research and development in encryption algorithms, quantum-resistant security, and AI-driven fraud detection will be crucial in sustaining the trust and reliability of card payment systems worldwide.

Keywords:
Card Payment Technology; Financial Security; EMV Chip and Contactless Payments; Fraud Prevention; Artificial Intelligence in Payments; Blockchain in Financial Services

1. INTRODUCTION

1.1 Background and Context

Before the advent of digital transactions, financial exchanges primarily relied on physical cash and barter systems. Cash transactions were the dominant means of payment, facilitating direct exchanges without the need for intermediaries. This system, while straightforward, had notable drawbacks, including risks of theft, counterfeiting, and inefficiencies in large-scale transactions [1]. The reliance on cash also made financial record-keeping cumbersome, with businesses and individuals struggling to maintain accurate and secure transaction histories. As economies expanded, the need for more efficient and secure payment methods became increasingly evident [2].

The transition from cash-based transactions to card payments marked a pivotal shift in financial systems. The introduction of charge cards in the mid-20th century allowed consumers to defer payments, leading to the development of credit cards by financial institutions. The emergence of magnetic stripe technology in the 1970s enhanced security and transaction processing speed, reducing the reliance on manual record-keeping [3]. By the 1990s, electronic payment terminals and chip-based cards revolutionized point-of-sale transactions, offering a higher level of security through encrypted authentication mechanisms [4]. With the rapid rise of e-commerce in the early 2000s, card payments became integral to global financial ecosystems, further emphasizing the necessity of robust security measures [5].

Security in financial transactions has always been paramount, given the increasing risks of fraud, identity theft, and cyberattacks. Early card payment systems were susceptible to skimming and cloning, prompting financial institutions to adopt enhanced security protocols such as EMV (Europay, Mastercard, and Visa) chip technology [6]. The introduction of tokenization and biometric authentication further strengthened security frameworks, reducing vulnerabilities associated with card-not-present transactions [7]. Regulatory bodies, including the Payment Card Industry Data Security Standard (PCI DSS), have played a critical role in ensuring compliance with security best practices, minimizing fraud risks across digital payment platforms [8]. As financial transactions continue evolving, the demand for advanced security solutions remains a focal point in ensuring the integrity and reliability of digital payment systems [9].

1.2 Research Objectives and Scope

The primary objective of this study is to analyze the evolution of card payment technology, focusing on its historical development, technological advancements, and security innovations. Understanding how card payments have progressed from basic charge cards to contactless and mobile transactions provides insights into the technological breakthroughs shaping the modern financial landscape [10]. Additionally, this research aims to assess the role of security measures in mitigating fraud and ensuring the trustworthiness of digital payment systems [11].

The scope of this study encompasses key security innovations such as end-to-end encryption, multi-factor authentication, and blockchain applications in payment systems. By examining fraud prevention strategies, including artificial intelligence-driven anomaly detection and behavioral biometrics, this study highlights how financial institutions combat cyber threats [12]. Furthermore, the research explores the impact of regulatory frameworks on card payment security, addressing compliance requirements imposed by global financial regulators [13]. The interplay between technological advancements and legal policies is critical in shaping secure payment infrastructures, ensuring both consumer protection and financial stability [14].

This article is structured into several sections to provide a comprehensive analysis. Following this introductory chapter, Section 2 delves into the historical evolution of payment systems, tracing the transition from cash transactions to digital payments. Section 3 examines security threats associated with card payments, identifying key risks and vulnerabilities. Section 4 explores technological advancements in fraud prevention, highlighting innovations that enhance transaction security. Section 5 discusses regulatory influences on payment security, assessing the role of compliance in mitigating fraud. Finally, Section 6 presents conclusions and future research directions, outlining potential advancements in secure payment technologies [15].

The research methodology employed in this study includes a review of existing literature, industry reports, and regulatory documents to provide a well-rounded perspective on payment security trends. A qualitative analysis of case studies involving financial institutions and payment service providers offers insights into real-world applications of security measures [16]. Through this approach, the study aims to contribute to the growing body of knowledge on digital payment security, offering valuable recommendations for enhancing transaction integrity and consumer trust [17].

2. THE EARLY STAGES OF CARD PAYMENT SYSTEMS

2.1 The Emergence of Payment Cards

The introduction of credit and charge cards in the mid-20th century marked a transformative shift in financial transactions. Charge cards, first introduced in the 1950s, allowed consumers to make purchases on credit, with the expectation of full repayment by the end of the billing cycle. Diners Club and American Express were among the pioneers in launching such cards, targeting affluent consumers and business travelers [5]. These early charge cards laid the foundation for modern credit cards, which emerged shortly thereafter with the introduction of revolving credit systems, enabling users to carry balances over multiple billing periods [6].

Financial institutions played a crucial role in the widespread adoption of payment cards. Banks recognized the potential of credit cards in expanding their customer base and improving transaction efficiency. By the 1970s, major banks such as Bank of America had developed their own credit card networks, leading to the establishment of globally recognized brands like Visa and Mastercard [7]. These financial institutions invested heavily in promoting card usage, partnering with merchants to create extensive payment acceptance networks. However, early adoption faced resistance from consumers unfamiliar with the concept of cashless transactions, necessitating marketing campaigns to build trust in the new payment method [8].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Security concerns were prevalent in early card transactions, primarily due to the absence of robust authentication mechanisms. The reliance on manual card imprints and signature verification made fraudulent activities relatively easy to execute. Criminals exploited weak verification processes to forge signatures and use stolen cards without detection [9]. Additionally, lost or stolen cards posed significant risks, as there were no immediate means to block unauthorized transactions. Financial institutions responded by introducing cardholder verification lists and hotlines for reporting lost cards, but these measures were insufficient in curbing fraud at scale [10]. As a result, the need for enhanced security technologies became increasingly apparent, prompting the development of more sophisticated payment card systems.

2.2 Magnetic Stripe Technology and Its Limitations

The adoption of magnetic stripe technology in the 1970s revolutionized payment card transactions. By embedding account information on a magnetic strip, banks and merchants could process payments electronically, reducing reliance on manual imprinting and signature verification [11]. This advancement enabled faster transaction processing and improved efficiency at retail locations, paving the way for widespread card usage across industries. Magnetic stripe cards became the standard for payment processing, providing a cost-effective solution for financial institutions and businesses seeking to modernize their operations [12].

Despite its advantages, magnetic stripe technology introduced new security vulnerabilities. One of the primary concerns was the ease of counterfeiting, as fraudsters developed techniques to clone card data using skimming devices. These devices, often discreetly installed on ATMs or point-of-sale terminals, could extract card information and replicate it onto counterfeit cards [13]. The rise of skimming-related fraud led to substantial financial losses for banks and merchants, prompting efforts to enhance transaction security. Another critical limitation was the static nature of the data stored on magnetic stripes, which made it susceptible to unauthorized duplication and reuse [14].

Before the advent of chip-based technology, financial institutions implemented several fraud prevention mechanisms to mitigate security risks associated with magnetic stripe cards. One approach was the introduction of daily transaction limits and spending thresholds to reduce exposure to fraudulent activities. Additionally, banks developed real-time fraud detection systems that analyzed spending patterns and flagged suspicious transactions for further review [15]. The implementation of PIN verification for ATM transactions added an extra layer of security, though it did not fully prevent fraudulent activities involving counterfeit cards [16]. Despite these efforts, the growing sophistication of financial criminals underscored the need for more secure authentication methods, ultimately leading to the development of EMV chip technology [17].

2.3 The Role of Regulations in Payment Card Security

The evolution of payment card security has been closely linked to the implementation of regulatory frameworks aimed at mitigating fraud and ensuring consumer protection. In the early stages of card-based transactions, security regulations were limited, with banks primarily relying on internal policies to address fraud risks. However, as financial crimes involving payment cards increased, regulators recognized the necessity of establishing industry-wide standards to enhance transaction security [18]. By the 1990s, financial regulatory bodies began introducing mandates requiring banks and merchants to implement fraud prevention measures, including stronger authentication protocols and data encryption techniques [19].

International financial institutions played a crucial role in standardizing security practices across global payment networks. Organizations such as the International Organization for Standardization (ISO) and the Payment Card Industry Security Standards Council (PCI SSC) developed security guidelines aimed at ensuring the integrity of card transactions. The ISO 7813 standard established specifications for payment cards, including data formatting and physical characteristics, while the PCI Data Security Standard (PCI DSS) mandated compliance with stringent security controls to protect cardholder information [20]. These regulatory efforts helped to create a more secure payment ecosystem, reducing fraud-related losses for financial institutions and consumers alike [21].

Compliance requirements have had a significant impact on the development of payment card technology. Regulations mandating the adoption of EMV chip technology, for example, have led to a substantial reduction in counterfeit card fraud by replacing static magnetic stripe data with dynamic authentication mechanisms [22]. Similarly, the introduction of Strong Customer Authentication (SCA) requirements under the revised Payment Services Directive (PSD2) has reinforced security in online transactions, necessitating multi-factor authentication for card-not-present payments [23]. While compliance with these regulations presents challenges for businesses in terms of implementation costs and operational adjustments, the long-term benefits of enhanced security and fraud reduction outweigh the initial investment [24].

As digital payment technologies continue to evolve, regulatory bodies remain instrumental in shaping security standards and addressing emerging threats. The increasing prevalence of artificial intelligence-driven fraud detection and blockchain-based transaction verification underscores the need for adaptive regulatory frameworks capable of keeping pace with technological advancements [25]. Moving forward, the alignment of security regulations with industry innovations will be crucial in maintaining the integrity of global payment systems while fostering consumer trust in digital transactions [26].

3. THE CHIP REVOLUTION: EMV AND ITS IMPACT

3.1 Introduction of EMV Technology

EMV (Europay, Mastercard, and Visa) technology was developed in response to the increasing prevalence of payment card fraud associated with magnetic stripe cards. Introduced in the mid-1990s, EMV aimed to provide a more secure alternative to traditional payment cards by embedding microprocessor chips capable of generating dynamic authentication codes for each transaction [9]. The adoption of EMV technology was driven by financial institutions and regulatory bodies seeking to enhance security in card-present transactions and mitigate risks related to counterfeiting and unauthorized card use [10].

The primary difference between magnetic stripe and chip-based cards lies in the method of data storage and transaction authentication. Magnetic stripe cards store static account information, making them susceptible to skimming, where fraudsters extract card data and create duplicates. In contrast, EMV chip cards use encrypted, dynamic authentication data that changes with every transaction, making duplication nearly impossible [11]. This dynamic nature significantly enhances transaction security, as unauthorized use of stolen card data is rendered ineffective without the physical chip and associated authentication methods [12].

Security improvements with chip-based cards extend beyond encryption. EMV transactions require cardholder verification methods such as PIN authentication or biometric validation, adding an extra layer of security [13]. Furthermore, the use of cryptographic keys prevents card data from being reused even if intercepted. These advancements have led to a substantial reduction in counterfeit card fraud and unauthorized in-person transactions, reinforcing consumer confidence in electronic payments [14]. As a result, many countries have mandated the adoption of EMV technology, positioning it as a global standard for secure payment processing [15].

3.2 Fraud Prevention and Liability Shifts

The widespread adoption of EMV technology has led to a significant reduction in card-present fraud. By replacing magnetic stripe cards with chip-enabled alternatives, financial institutions have effectively minimized the risk of counterfeit fraud, which was previously one of the most common forms of payment fraud [16]. Countries that transitioned to EMV early, such as the United Kingdom and Canada, experienced notable declines in fraud-related losses, reinforcing the technology's effectiveness in securing transactions [17].

A major development accompanying EMV adoption was the introduction of liability shifts in fraud cases. Before EMV, banks and card issuers primarily bore the costs of fraudulent transactions. However, liability shifts implemented by major payment networks transferred responsibility to the party with the weaker security infrastructure. Merchants who failed to upgrade to EMV-compliant systems became liable for fraudulent transactions occurring on non-EMV terminals [18]. This shift incentivized merchants to adopt chip-based payment solutions, reducing overall fraud risks across the payment ecosystem [19].

Despite its benefits, global adoption of EMV technology faced several challenges. Developing countries encountered financial and logistical obstacles in upgrading payment infrastructure, slowing adoption rates [20]. Additionally, some merchants hesitated to transition due to the costs associated with upgrading terminals and retraining staff. Resistance was also observed in markets where contactless and mobile payment solutions gained traction, leading some businesses to prioritize alternative payment security measures over full EMV implementation [21]. Nevertheless, as digital fraud threats continue to evolve, EMV remains a cornerstone in securing in-person payment transactions worldwide [22].

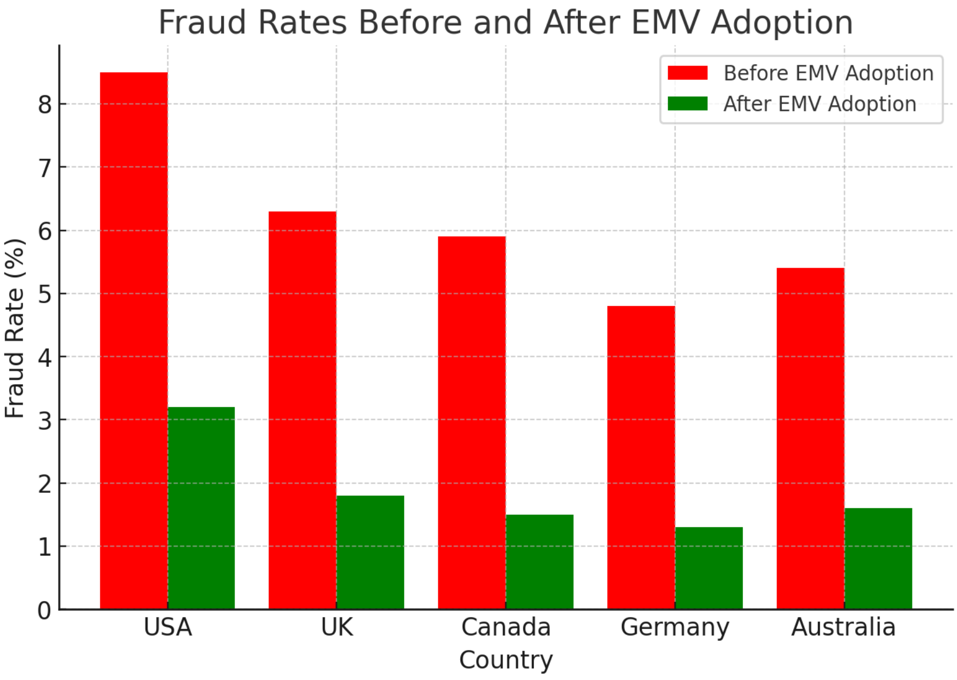
3.3 The Role of Tokenization in Enhancing Security

Tokenization is a security mechanism that replaces sensitive payment information with a unique, randomly generated identifier, or token, that has no exploitable value if intercepted. This technology ensures that payment card data is never directly exposed during transactions, reducing the risk of fraud and unauthorized access [23]. Tokenization is widely implemented across online transactions, mobile payments, and digital wallets, offering an additional layer of security beyond traditional encryption techniques [24].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

One of the key use cases of tokenization is in online transactions, where cybercriminals frequently target payment data. By substituting card numbers with tokens, e-commerce platforms prevent attackers from gaining access to usable payment details in the event of a data breach [25]. Similarly, tokenization plays a crucial role in mobile payment solutions such as Apple Pay and Google Pay, where device-specific tokens ensure that actual card information is never stored on mobile devices or transmitted during transactions [26]. This enhances security in contactless payments, mitigating risks associated with card cloning and skimming attacks [27].

The effectiveness of tokenization in reducing fraud risks is evident in its widespread adoption across financial institutions and payment processors. Unlike traditional encryption methods, which require decryption at some point in the transaction process, tokenization eliminates the need to store or transmit real card details, significantly reducing the attack surface for cybercriminals [28]. Furthermore, tokens can be limited to specific merchants, devices, or transaction types, providing an additional layer of fraud prevention. This dynamic approach to security has positioned tokenization as a critical component in the evolving landscape of digital payment protection [29].



3.4 Figure 1 Graph Comparing Fraud Reduction Pre- and Post-EMV Implementation

Fraud Reduction Trends Before and After EMV Adoption

To illustrate the impact of EMV technology on fraud reduction, the following figure presents a comparative analysis of fraudulent transaction rates before and after widespread EMV implementation.

3.5 EMV's Influence on Consumer and Merchant Adoption

The adoption of EMV technology among consumers and merchants has varied based on factors such as awareness, convenience, and perceived security benefits. Initially, some consumers resisted EMV due to unfamiliarity with chip-based transactions and longer processing times compared to traditional swipe methods [30]. However, as awareness of fraud prevention benefits grew, consumer adoption increased, particularly in regions where banks and regulators actively promoted the transition to EMV cards [31].

For merchants, the transition to EMV-compliant systems presented financial and operational challenges. Upgrading point-of-sale terminals required significant investment, particularly for small businesses with limited resources [32]. Additionally, merchants had to train staff on new transaction processes and adapt to consumer preferences for faster, contactless payment options. Despite these challenges, regulatory mandates and liability shifts eventually encouraged widespread adoption, positioning EMV as a fundamental component of secure financial transactions worldwide [33].

4. THE RISE OF CONTACTLESS AND MOBILE PAYMENTS

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

4.1 Evolution of Contactless Payment Technology

The development of Near Field Communication (NFC) technology has played a crucial role in revolutionizing contactless payments. NFC, a short-range wireless communication technology, enables secure exchanges of payment credentials between devices, allowing transactions to be completed with minimal physical interaction [12]. Originally developed for data exchange in transportation and access control systems, NFC quickly gained traction in financial services due to its speed and security advantages over traditional payment methods [13].

Tap-and-go payments, enabled by NFC technology, have significantly improved transaction efficiency and convenience. Unlike chip-and-PIN transactions, which require card insertion and user authentication, contactless payments allow users to simply tap their card or mobile device on an NFC-enabled terminal. This reduces transaction times and minimizes congestion at checkout points, benefiting both consumers and merchants [14]. Contactless transactions have been widely adopted in public transport systems, retail stores, and quick-service restaurants, where speed is a key factor in customer experience [15].

Security features in contactless transactions address concerns regarding unauthorized usage and fraud. Unlike magnetic stripe cards, which store static data, NFC transactions utilize dynamic authentication protocols, ensuring that each transaction generates a unique cryptographic code that cannot be reused [16]. Additionally, contactless cards and mobile wallets incorporate spending limits and proximity-based authentication to prevent long-range interception and unauthorized transactions [17]. Financial institutions have also introduced real-time fraud monitoring systems that detect suspicious spending patterns, adding an extra layer of security to contactless transactions [18].

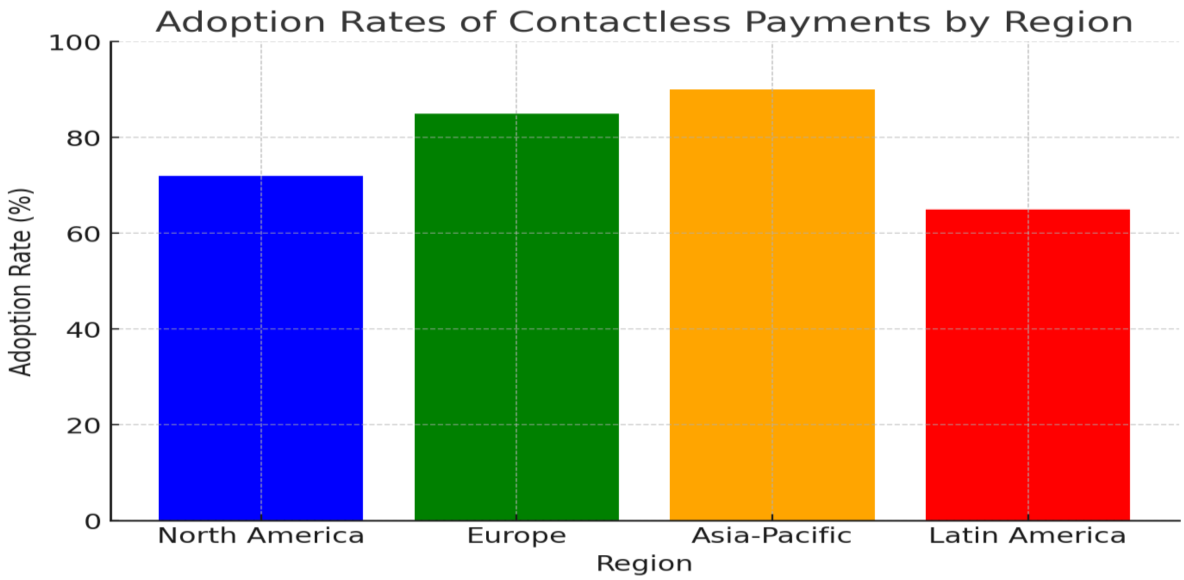
4.2 Mobile Wallets and Digital Payment Innovations

Mobile wallets, such as Apple Pay, Google Pay, and Samsung Pay, have expanded the functionality of contactless payments by integrating NFC technology with smartphone applications. These digital payment solutions allow users to store multiple payment cards securely on their devices, eliminating the need for physical wallets [19]. The widespread availability of NFC-enabled smartphones has accelerated the adoption of mobile wallets, making digital transactions more accessible to consumers worldwide [20].

One of the key advancements in mobile payment security is the integration of biometric authentication. Technologies such as fingerprint recognition, facial recognition, and iris scanning provide an additional layer of verification, ensuring that only authorized users can initiate transactions [21]. Unlike PIN-based authentication, which can be compromised through observation or data breaches, biometric authentication relies on unique physical traits that are difficult to replicate or steal [22]. These security enhancements have contributed to the growing trust in mobile payment solutions among consumers and businesses alike [23].

Despite advancements in security, mobile payments face several challenges. Cybercriminals have developed sophisticated techniques to exploit vulnerabilities in mobile payment ecosystems, including SIM swapping, malware attacks, and phishing schemes [24]. Additionally, the reliance on internet connectivity for mobile transactions exposes users to risks associated with unsecured networks and data interception [25]. To mitigate these threats, financial institutions continuously update encryption protocols and implement multi-factor authentication measures to safeguard mobile payment environments [26].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/



4.3 Figure 2 Adoption Trends of Contactless Payments by Region

Global Trends in Contactless Payment Adoption

To illustrate the growth of contactless payment adoption, the following figure presents a comparative analysis of contactless payment usage across different regions.

4.4 Challenges in Implementing Contactless Payments

Despite the widespread adoption of contactless payments, concerns over fraud remain a significant challenge. Contactless payment fraud, although lower than traditional card fraud, has been exploited by criminals through relay attacks, where hackers intercept NFC signals to execute unauthorized transactions [27]. Additionally, stolen or lost contactless cards can be used for small transactions before the cardholder reports the loss, leading to financial risks for consumers and financial institutions [28]. However, banks have implemented security measures such as transaction monitoring, spending caps, and liability protections to minimize fraudulent activities in contactless transactions [29].

Merchant adoption barriers and technology costs also hinder the expansion of contactless payment systems. While large retailers have embraced contactless terminals, smaller businesses often struggle with the cost of upgrading payment infrastructure. The initial investment in NFC-enabled point-of-sale (POS) terminals and ongoing maintenance costs can be prohibitive for small businesses operating on thin margins [30]. Furthermore, some merchants remain hesitant to transition to contactless payments due to concerns over processing fees and integration complexities with existing financial systems [31].

Consumer trust in mobile and contactless payment systems varies by region and demographic factors. While younger consumers are more inclined to adopt digital payment methods, older generations often exhibit resistance due to concerns over data privacy and security [32]. High-profile data breaches and cyberattacks have fueled skepticism about the safety of digital transactions, prompting regulatory bodies to enforce stricter compliance measures for payment security [33]. Financial institutions and technology providers continue to educate consumers on the benefits and safety of contactless payments to foster broader adoption and trust in digital payment ecosystems [34].

4.5 The Future of Contactless Payment Security

Advancements in secure element (SE) technology are expected to further enhance the security of contactless payments. Secure elements, which are tamper-resistant chips embedded in smartphones and payment cards, provide an isolated environment for storing sensitive payment credentials [35]. Emerging technologies such as embedded Secure Elements (eSE) and cloud-based secure elements offer enhanced protection against unauthorized access, ensuring that payment data remains secure across different devices and transaction environments [36].

Artificial intelligence (AI) plays an increasingly important role in fraud detection for contactless transactions. Machine learning algorithms analyze vast amounts of transaction data in real time, identifying abnormal spending patterns and flagging potentially fraudulent activities [37]. AI-driven fraud detection systems continuously adapt to evolving cyber threats, providing proactive security measures that mitigate risks before they escalate. As AI technology advances, financial institutions will increasingly rely on predictive analytics and behavioral analysis to enhance the security of contactless payment systems [38].

5. BIOMETRIC AND AI-DRIVEN SECURITY IN CARD PAYMENTS

5.1 Biometric Authentication in Card Payments

The integration of biometric authentication in card payments represents a significant advancement in financial security. Fingerprint and facial recognition technologies have emerged as reliable methods for verifying cardholders' identities, reducing reliance on traditional authentication mechanisms such as PINs and passwords [15]. Biometric payment cards, equipped with embedded fingerprint sensors, enable secure transactions by requiring user authentication before authorizing payments. Similarly, facial recognition systems, widely adopted in mobile payment applications, offer a seamless and secure alternative to traditional card-based transactions [16].

Biometrics enhance fraud prevention by linking transactions directly to the cardholder's unique physiological characteristics, making unauthorized access significantly more difficult. Unlike passwords or PINs, which can be stolen or guessed, biometric data is inherently unique and difficult to replicate [17]. This technology effectively mitigates card-present fraud, as even if a payment card is lost or stolen, unauthorized individuals cannot use it without biometric verification. Additionally, biometric authentication reduces the risk of identity theft in online transactions by introducing multi-factor authentication methods that require both biometric data and device-based authentication [18].

Despite its security advantages, biometric authentication raises regulatory concerns regarding data privacy and compliance. Financial institutions must adhere to stringent data protection laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which govern the collection, storage, and processing of biometric information [19]. Ensuring compliance with these regulations requires robust encryption protocols and secure data storage solutions to prevent unauthorized access to biometric databases. Moreover, regulators emphasize the need for user consent and transparency in biometric authentication systems to protect consumer rights and maintain trust in financial services [20].

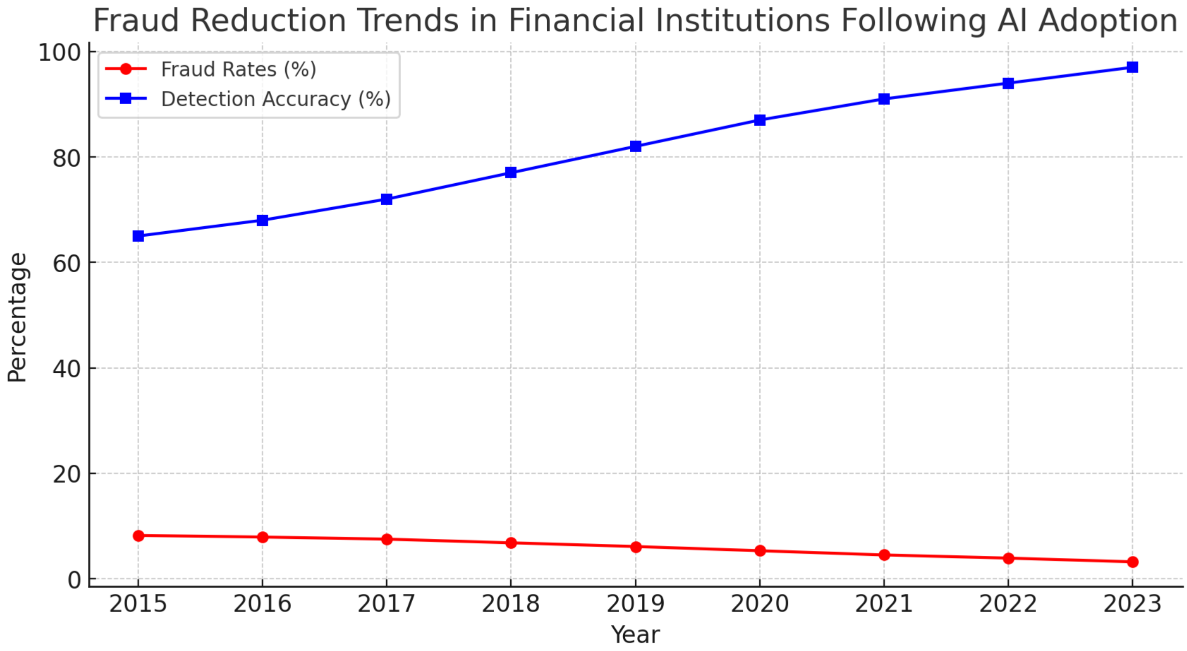
5.2 Artificial Intelligence in Fraud Detection

Artificial intelligence (AI) has become a critical tool in fraud detection, enabling financial institutions to identify and mitigate fraudulent transactions in real time. Machine learning algorithms analyze vast datasets, recognizing transaction patterns and detecting anomalies indicative of fraudulent activity [21]. Unlike rule-based fraud detection systems, AI-driven models continuously adapt to emerging threats, improving their accuracy in identifying suspicious behaviors and reducing false positives in fraud detection processes [22].

Several financial institutions have successfully implemented AI-driven security measures to combat fraud. For example, banks utilize AI-powered transaction monitoring systems that analyze user spending patterns and flag deviations that may indicate unauthorized activity [23]. Additionally, AI-enhanced fraud detection systems integrate behavioral biometrics, such as typing speed and touchscreen interactions, to differentiate between legitimate users and fraudsters attempting to gain unauthorized access [24]. These advancements have led to substantial reductions in fraud-related losses and improved fraud detection accuracy in banking and payment ecosystems [25].

Despite its effectiveness, AI adoption in fraud detection presents challenges for financial institutions. One of the primary obstacles is the requirement for high-quality data to train AI models effectively. Poorly curated or biased datasets can lead to inaccurate fraud detection, increasing the risk of false positives or missed fraudulent transactions [26]. Moreover, AI models must be continuously updated to keep pace with evolving cyber threats, requiring significant investment in infrastructure and expertise. Regulatory compliance also poses challenges, as financial institutions must ensure that AI-driven decision-making processes adhere to transparency and fairness standards to prevent unintended biases in fraud detection [27].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/



5.3 Figure 3 AI's Impact on Fraud Detection and Reduction Rates

Impact of AI-Driven Fraud Detection Systems on Fraud Reduction

To illustrate the effectiveness of AI in combating fraud, the following figure presents a comparative analysis of fraud detection accuracy and fraud reduction rates before and after the implementation of AI-driven security measures.

5.4 Challenges in Biometric and AI Adoption

While biometric authentication and AI-driven fraud detection offer significant security benefits, their adoption faces several challenges. One of the primary concerns is consumer apprehension regarding privacy and data security. Many consumers express hesitancy in sharing biometric data with financial institutions due to fears of misuse, data breaches, and lack of control over personal information [28]. Addressing these concerns requires transparent communication regarding data handling practices, as well as the implementation of secure storage and encryption techniques to protect biometric data from unauthorized access [29].

Technological barriers also impact the scalability of AI-driven security solutions. Implementing AI fraud detection systems requires sophisticated infrastructure capable of processing large volumes of transactional data in real time [30]. Smaller financial institutions may struggle with the costs associated with deploying AI-based security measures, limiting their ability to combat fraud effectively. Additionally, AI models must undergo rigorous testing to ensure their accuracy and reliability, requiring substantial computational resources and technical expertise [31].

Balancing security with user convenience remains a critical challenge in biometric payments. While biometrics enhance security, they can also introduce friction in the payment process if authentication methods are slow or unreliable. For example, fingerprint recognition may fail under certain conditions, such as wet or damaged fingertips, leading to transaction delays [32]. Similarly, facial recognition systems may struggle in low-light environments or with facial obstructions, impacting user experience. To address these issues, financial institutions continue to refine biometric authentication systems, incorporating multi-modal authentication methods that combine different biometric modalities for greater reliability [33].

As financial technology continues to evolve, striking a balance between security and usability will be essential in driving widespread adoption of biometric authentication and AI-driven fraud detection solutions in the payment industry [34].

6. THE ROLE OF REGULATORY COMPLIANCE IN PAYMENT SECURITY

6.1 PCI DSS and Its Influence on Payment Security

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized framework designed to enhance the security of card transactions by establishing comprehensive data protection requirements. Introduced in 2004 by major payment networks, including Visa, Mastercard, and American Express, PCI DSS aims to safeguard cardholder data through strict security protocols [19]. The standard applies to all entities involved in payment processing, including merchants, payment processors, and financial institutions, ensuring a consistent approach to securing card transactions and preventing unauthorized data access [20].

PCI DSS guidelines shape card payment security by mandating encryption, network segmentation, and access control measures to protect sensitive financial information. Organizations must implement multi-layered security strategies, such as tokenization and end-to-end encryption, to minimize the risk of data breaches and card fraud [21]. Additionally, PCI DSS compliance requires regular vulnerability assessments, penetration testing, and employee training to mitigate security threats effectively. These measures have significantly contributed to reducing payment card fraud and enhancing consumer trust in digital transactions [22].

However, compliance with PCI DSS presents challenges, particularly for small businesses and fintech firms. The cost of implementing security controls, such as secure payment gateways and encryption technologies, can be prohibitive for smaller enterprises with limited resources [23]. Additionally, the complexity of compliance requirements often necessitates expert assistance, further increasing operational costs. Many fintech startups, which rely on agile development processes, struggle to balance regulatory adherence with innovation, highlighting the need for scalable security solutions tailored to smaller entities [24].

6.2 Open Banking and Its Security Implications

Open banking is a financial innovation that enables third-party providers (TPPs) to access banking data through application programming interfaces (APIs), facilitating seamless digital transactions and personalized financial services. This model fosters competition and enhances consumer convenience by allowing users to aggregate financial accounts, initiate payments, and access tailored financial insights from multiple providers [25]. Supported by regulatory initiatives such as the European Union’s Revised Payment Services Directive (PSD2), open banking has transformed the financial landscape by promoting transparency and innovation in payment systems [26].

Despite its benefits, open banking introduces security risks, including unauthorized data access, API vulnerabilities, and fraud. The exposure of sensitive financial information to third-party providers increases the risk of data breaches, necessitating robust authentication mechanisms such as strong customer authentication (SCA) and OAuth-based authorization protocols [27]. Additionally, cybercriminals exploit weak API security configurations to intercept and manipulate transaction requests, highlighting the importance of secure coding practices and continuous security monitoring in open banking ecosystems [28].

Regulatory frameworks play a critical role in securing open banking transactions. PSD2 mandates financial institutions to implement secure API standards, ensuring that third-party providers undergo rigorous authentication and compliance checks before accessing banking data [29]. Similarly, data protection laws such as the General Data Protection Regulation (GDPR) establish guidelines for handling and storing consumer financial data, emphasizing transparency and user consent [30]. As open banking adoption expands globally, regulatory bodies continue refining security policies to address emerging threats while fostering innovation in financial services [31].

6.3 Table 2 Comparison of Major Regulatory Frameworks in Payment Security

The following table provides a comparative overview of major regulatory frameworks governing payment security, highlighting their scope, primary security measures, and compliance requirements.

Regulatory Framework	**Applicability**	**Key Security Provisions**	**Enforcement Mechanisms**
PCI DSS (Payment Card Industry Data Security Standard)	Applies to all entities handling card transactions, including merchants, payment processors, and financial institutions.	Requires encryption of cardholder data, access controls, network monitoring, and regular security assessments.	Enforced by major payment card networks (Visa, Mastercard, etc.), non-compliance may result in fines, higher transaction fees, or revocation of payment processing privileges.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Regulatory Framework	Applicability	Key Security Provisions	Enforcement Mechanisms
GDPR (General Data Protection Regulation)	Applies to any organization processing personal data of EU residents, including financial institutions handling payment data.	Mandates strict data protection measures, encryption of sensitive information, user consent requirements, and the right to data erasure.	Enforced by national data protection authorities across the EU; non-compliance can lead to fines of up to 4% of global annual revenue or €20 million, whichever is higher.
PSD2 (Revised Payment Services Directive)	Governs banks, payment service providers, and third-party financial institutions operating within the EU.	Implements Strong Customer Authentication (SCA), open banking API security, and mandates secure communication between banks and third-party providers.	Enforced by financial regulators in EU member states, with penalties for non-compliance, including restrictions on financial operations and significant fines.

6.4 The Role of Central Banks and Financial Authorities

Government bodies and financial authorities play a crucial role in shaping payment security regulations by establishing policies that enhance transaction integrity and protect consumers. Central banks and financial regulators oversee the implementation of security standards, ensuring that financial institutions and payment service providers comply with risk management guidelines to mitigate fraud and cyber threats [32]. By enforcing anti-money laundering (AML) regulations and Know Your Customer (KYC) policies, regulators strengthen the security of digital payment ecosystems, reducing illicit financial activities [33].

The emergence of central bank digital currencies (CBDCs) has introduced new dimensions to payment security. Unlike traditional digital transactions, which rely on commercial bank networks, CBDCs are issued and regulated directly by central banks, providing enhanced oversight and security measures [34]. CBDCs leverage blockchain technology and cryptographic security protocols to prevent counterfeiting and unauthorized access, offering a secure alternative to conventional card payments. Additionally, CBDC implementation enables real-time transaction tracking, reducing financial crime risks and enhancing transparency in digital payments [35].

Future directions in financial regulations for card payments will likely focus on strengthening cybersecurity resilience and adapting to emerging payment technologies. Regulatory authorities are expected to introduce enhanced compliance frameworks that incorporate artificial intelligence-driven fraud detection and real-time risk assessment mechanisms [36]. Moreover, cross-border regulatory collaboration will become increasingly important as digital payments continue to expand globally, requiring standardized security protocols to ensure interoperability and fraud prevention across jurisdictions [37]. As payment technologies evolve, financial authorities must balance regulatory oversight with innovation, fostering a secure and efficient digital financial ecosystem [38].

7. THE FUTURE OF CARD PAYMENT SECURITY: TRENDS AND INNOVATIONS

7.1 Blockchain Technology in Secure Payments

Blockchain technology has introduced a decentralized security model that enhances the security and transparency of card payments. Unlike traditional payment systems, which rely on centralized intermediaries such as banks and payment processors, blockchain enables peer-to-peer transactions that are recorded on an immutable distributed ledger [22]. This decentralized approach reduces the risk of fraud and unauthorized modifications by ensuring that each transaction is cryptographically verified and permanently stored across multiple nodes in a blockchain network [23].

Blockchain-based tokenization has further strengthened secure transactions by replacing sensitive payment information with unique digital tokens. Unlike conventional tokenization, which relies on a centralized entity to generate and store tokens, blockchain-based tokenization distributes encrypted transaction records across multiple nodes, reducing the risk of data breaches [24]. Additionally, smart contracts—self-executing agreements programmed on blockchain networks—enhance security by automating transaction validation processes and reducing human intervention in payment settlements [25].

Despite its potential benefits, blockchain adoption in mainstream finance faces several challenges. The scalability of blockchain networks remains a major concern, as high transaction volumes can lead to network congestion and increased processing times [26]. Additionally, regulatory uncertainty surrounding blockchain-based payments has hindered widespread adoption, as financial authorities continue to assess compliance requirements and anti-money laundering measures for decentralized financial transactions [27]. Furthermore, the integration of blockchain with existing payment infrastructure requires significant technological investment, which may limit adoption among traditional financial institutions [28].

7.2 The Integration of Quantum Computing in Financial Security

Quantum computing presents both opportunities and threats to financial security, particularly in the realm of encryption. Current cryptographic models, such as RSA and ECC, rely on complex mathematical problems that classical computers struggle to solve. However, quantum computers possess the computational power to break these encryption models, posing a significant risk to the security of payment systems [29]. If quantum computing advances at its current pace, existing cryptographic frameworks could become obsolete, exposing card transactions and digital payments to unprecedented security threats [30].

To mitigate these risks, researchers are developing quantum-resistant security models capable of withstanding attacks from quantum computers. Post-quantum cryptography (PQC) algorithms, such as lattice-based encryption and hash-based signatures, offer enhanced security by utilizing mathematical problems that remain computationally infeasible even for quantum processors [31]. Financial institutions are actively exploring the implementation of PQC in payment security frameworks to future-proof digital transactions against quantum threats [32].

In addition to quantum-resistant cryptography, innovations in cryptographic security for financial transactions are advancing rapidly. Quantum key distribution (QKD) enables ultra-secure communication by leveraging the principles of quantum mechanics to ensure that encryption keys cannot be intercepted without detection [33]. This technology has the potential to revolutionize financial security by providing an unbreakable encryption mechanism for card payments and online transactions. As quantum computing capabilities evolve, financial organizations must prioritize investment in quantum-secure technologies to maintain the integrity of digital payment systems [34].

7.3 The Next Generation of Smart Payment Cards

The evolution of smart payment cards has introduced dynamic CVV (Card Verification Value) and biometric authentication features to enhance security. Unlike traditional static CVV codes, which remain unchanged, dynamic CVV technology generates a new verification code for each transaction, reducing the risk of fraud resulting from stolen card details [35]. Additionally, biometric authentication payment cards integrate fingerprint recognition directly into the card, allowing users to authenticate transactions securely without relying on PIN codes or signatures [36]. These innovations aim to combat card-not-present fraud and strengthen user authentication in card-based transactions.

The integration of the Internet of Things (IoT) with payment cards is further enhancing transaction security. IoT-enabled payment cards utilize embedded microchips and wireless communication protocols to enable real-time fraud detection and remote card deactivation in case of security threats [37]. Some advanced payment cards are equipped with near-field communication (NFC) and Bluetooth capabilities, allowing secure interactions with IoT devices such as smart wallets and biometric authentication terminals [38]. These features provide enhanced security measures while maintaining user convenience in digital transactions.

Consumer adoption trends for smart payment technologies indicate a growing demand for enhanced security and seamless transaction experiences. A significant portion of consumers express willingness to adopt biometric authentication cards, citing increased security and ease of use as primary factors [39]. However, concerns over privacy, data storage, and potential misuse of biometric information remain barriers to widespread adoption. Financial institutions are addressing these concerns by implementing strong encryption protocols and ensuring compliance with data protection regulations to build consumer trust in next-generation payment technologies [40].

7.4 Table 3 Emerging Payment Security Technologies and Their Potential Impact

The following table provides an overview of innovative payment security technologies, highlighting their functionalities and potential impact on the financial industry.

Technology	Security Enhancements	Industry Adoption Potential
Blockchain-Based Tokenization	Decentralized ledger reduces fraud risks, tokenization replaces sensitive card data with encrypted tokens.	Increasing adoption in financial services, particularly in cross-border payments and fraud prevention.

IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Technology	Security Enhancements	Industry Adoption Potential
Quantum-Resistant Encryption	Utilizes post-quantum cryptographic algorithms to withstand attacks from quantum computers.	Still in early research stages; financial institutions are exploring integration into security frameworks.
IoT-Enabled Payment Cards	Integrates biometric authentication, dynamic CVV, and real-time fraud detection via connected networks.	Gaining traction with major payment networks and smart card manufacturers, especially for high-security transactions.

8. CONCLUSION

8.1 Summary of Key Innovations in Card Payment Security

The evolution of card payment security has been marked by continuous technological advancements aimed at reducing fraud and enhancing transaction integrity. The transition from magnetic stripe cards to more secure alternatives, such as EMV chip technology and biometric authentication, has significantly strengthened financial security. Magnetic stripe cards, while convenient, were highly susceptible to skimming and duplication, leading to widespread fraud. The introduction of EMV chips improved security by using dynamic authentication protocols that made counterfeiting more difficult. Further advancements, such as dynamic CVV codes and biometric authentication, have further fortified payment security, ensuring that only authorized users can complete transactions.

Contactless and mobile payment technologies have also contributed to this transformation, integrating tokenization and real-time fraud monitoring to protect cardholder data. The emergence of blockchain-based security models and quantum-resistant encryption represents the next frontier in safeguarding digital payments. Additionally, AI-driven fraud detection systems have enabled financial institutions to proactively identify suspicious transactions, reducing fraud-related financial losses.

Security innovations have played a crucial role in shaping consumer trust in financial services. Consumers are more likely to adopt digital payment solutions when they perceive transactions as secure and reliable. The implementation of strong authentication measures, regulatory compliance standards, and transparent data protection policies has reinforced confidence in electronic transactions. Financial institutions must continue prioritizing security advancements to maintain consumer trust and mitigate emerging threats in the rapidly evolving payment landscape.

8.2 Challenges and Limitations in Securing Card Payments

Despite significant progress in card payment security, several challenges persist. Fraud risks continue to evolve, with cybercriminals employing sophisticated techniques such as social engineering, malware attacks, and AI-driven fraud schemes to exploit vulnerabilities in payment systems. Card-not-present fraud remains a major concern, particularly in e-commerce transactions, where attackers bypass traditional authentication measures. Even with biometric and tokenization advancements, new attack vectors emerge, requiring continuous adaptation of security strategies.

Compliance challenges and regulatory gaps present additional hurdles in securing financial transactions. While frameworks such as PCI DSS, GDPR, and PSD2 establish security guidelines, inconsistencies in implementation across regions create loopholes that cybercriminals can exploit. Small businesses and fintech startups often struggle with the financial and technical burdens of compliance, leaving them more vulnerable to attacks. Additionally, the rapid evolution of financial technologies often outpaces regulatory updates, creating uncertainty regarding best practices and enforcement mechanisms. Addressing these challenges requires a collaborative effort between financial institutions, regulatory bodies, and technology providers to ensure security measures remain effective and adaptable.

8.3 Future Research and Policy Recommendations

Further research is needed to explore AI-driven payment security solutions, particularly in fraud detection and real-time threat mitigation. Machine learning models can enhance predictive analytics, identifying fraudulent patterns before transactions are completed. However, research must focus on improving the accuracy of AI models, minimizing false positives, and ensuring transparency in automated decision-making processes. Additionally, integrating AI with blockchain and quantum-resistant encryption could enhance the security of digital transactions, providing long-term solutions against evolving cyber threats.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

From a policy perspective, regulatory frameworks should be continuously updated to align with emerging security risks and technological advancements. Governments and financial regulators must collaborate with industry stakeholders to develop standardized security guidelines that facilitate global interoperability while maintaining strong consumer protections. Policies should also encourage financial inclusion by ensuring that security compliance requirements do not disproportionately burden small businesses and emerging fintech enterprises. Investing in consumer education initiatives will also be essential, helping individuals recognize and avoid potential fraud risks while navigating the digital payment ecosystem. By fostering innovation alongside regulatory oversight, the financial sector can maintain a secure and resilient payment infrastructure for the future.

REFERENCE

1. Gomber P, Kauffman RJ, Parker C, Weber BW. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of management information systems. 2018 Jan 2;35(1):220-65.
2. Frame WS, White LJ. Technological change, financial innovation, and diffusion in banking. The Oxford handbook of banking. 2014 Nov 27:486-507.
3. Kang J. Mobile payment in Fintech environment: trends, security challenges, and services. Human-centric Computing and Information sciences. 2018 Oct 30;8(1):32.
4. Au YA, Kauffman RJ. The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. Electronic commerce research and applications. 2008 Jun 1;7(2):141-64.
5. Drew SA. Accelerating innovation in financial services. Long range planning. 1995 Aug 1;28(4):1-21.
6. Dapp T, Slomka L, AG DB, Hoffmann R. Fintech–The digital (r) evolution in the financial sector. Deutsche Bank Research. 2014 Nov 11;11:1-39.
7. Anderson R, Bond M, Choudary O, Murdoch SJ, Stajano F. Might financial cryptography kill financial innovation?–the curious case of EMV. InInternational Conference on Financial Cryptography and Data Security 2011 Feb 28 (pp. 220-234). Berlin, Heidelberg: Springer Berlin Heidelberg.
8. King B. Bank 2.0: How customer behaviour and technology will change the future of financial services. Brett King; 2010.
9. Stewart H, Jürjens J. Data security and consumer trust in FinTech innovation in Germany. Information & Computer Security. 2018 Mar 12;26(1):109-28.
10. Furst K, Lang WW, Nolle DE. Technological innovation in banking and payments: industry trends and implications for banks. Quarterly Journal, Office of the Comptroller of the Currency. 1998 Sep 1;17(3):23.
11. Bezhovski Z. The future of the mobile payment as electronic payment system. European Journal of Business and Management. 2016;8(8).
12. Fain D, Roberts ML. Technology vs. consumer behavior: the battle for the financial services customer. Journal of Direct Marketing. 1997 Jan 1;11(1):44-54.
13. Arner DW, Barberis J, Buckley RP. The evolution of Fintech: A new post-crisis paradigm. Geo. J. Int'l L.. 2015;47:1271.
14. Dapp TF, Stobbe A, Wruuck P, Keane B, Napier J, Sabadra A, Yamada Y, Speyer B, AG DB, Hoffmann R. The future of (mobile) payments [Internet]. 2012
15. Furst K, Nolle DE. Technological innovation in retail payments: Key developments and implications for banks. Capco Institute Journal of Financial Transformation. 2004 Dec 1(12):93.
16. Arvidsson N. Consumer attitudes on mobile payment services–results from a proof of concept test. International Journal of Bank Marketing. 2014 Apr 1;32(2):150-70.
17. Khan BU, Olanrewaju RF, Baba AM, Langoo AA, Assad S. A compendious study of online payment systems: Past developments, present impact, and future considerations. International journal of advanced computer science and applications. 2017;8(5).
18. Barras R. Interactive innovation in financial and business services: The vanguard of the service revolution. Research policy. 1990 Jun 1;19(3):215-37.
19. Lim SH, Kim DJ, Hur Y, Park K. An empirical study of the impacts of perceived security and knowledge on continuous intention to use mobile fintech payment services. International Journal of Human–Computer Interaction. 2019 Jun 15;35(10):886-98.
20. Cronin MJ. Banking and Finance on the Internet. John Wiley & Sons; 1998.

21. Karnouskos S. Mobile payment: a journey through existing procedures and standardization initiatives. IEEE Communications Surveys & Tutorials. 2004 Oct 1;6(4):44-66.
22. Shahrokhi M. E-finance: status, innovations, resources and future challenges. Managerial Finance. 2008 May 9;34(6):365-98.
23. Ondrus J, Pigneur Y. Towards a holistic analysis of mobile payments: A multiple perspectives approach. Electronic commerce research and applications. 2006 Sep 1;5(3):246-57.
24. Ali R, Barrdear J, Clews R, Southgate J. Innovations in payment technologies and the emergence of digital currencies. Bank of England Quarterly Bulletin. 2014 Sep 16:Q3.
25. Aduda J, Kingoo N. The relationship between electronic banking and financial performance among commercial banks in Kenya. Journal of finance and investment analysis. 2012;1(3):99-118.
26. He MD, Leckow MR, Haksar MV, Griffoli MT, Jenkinson N, Kashima MM, Khiaonarong T, Rochon MC, Tourpe H. Fintech and financial services: Initial considerations. International Monetary Fund; 2017 Jun 19.
27. Devlin JF. Technology and innovation in retail banking distribution. International Journal of Bank Marketing. 1995 Jun 1;13(4):19-25.
28. Mallat N, Rossi M, Tuunainen VK. Mobile banking services. Communications of the ACM. 2004 May 1;47(5):42-6.
29. Cortet M, Rijks T, Nijland S. PSD2: The digital transformation accelerator for banks. Journal of Payments Strategy & Systems. 2016 Mar 1;10(1):13-27.
30. Guo Y, Liang C. Blockchain application and outlook in the banking industry. Financial innovation. 2016 Dec 9;2(1):24.
31. Romānova I, Kudinska M. Banking and fintech: A challenge or opportunity?. InContemporary issues in finance: Current challenges from across Europe 2016 Nov 22 (Vol. 98, pp. 21-35). Emerald Group Publishing Limited.
32. Duncombe R, Boateng R. Mobile Phones and Financial Services in Developing Countries: a review of concepts, methods, issues, evidence and future research directions. Third World Quarterly. 2009 Oct 1;30(7):1237-58.
33. Duffie D, Rahi R. Financial market innovation and security design: An introduction. Journal of Economic Theory. 1995 Feb 1;65(1):1-42.
34. Sohail MS, Shanmugham B. E-banking and customer preferences in Malaysia: An empirical investigation. Information sciences. 2003 Apr 1;150(3-4):207-17.
35. Gomber P, Koch JA, Siering M. Digital Finance and FinTech: current research and future research directions. Journal of business economics. 2017 Jul;87:537-80.
36. Poon WC. Users' adoption of e-banking services: the Malaysian perspective. Journal of business & industrial marketing. 2007 Dec 24;23(1):59-69.
37. Saksonova S, Kuzmina-Merlino I. Fintech as financial innovation–The possibilities and problems of implementation.
38. Dermine J. Digital banking and market disruption: a sense of déjà vu. Financial Stability Review. 2016 Apr;20:17-23.
39. Shim Y, Shin DH. Analyzing China's fintech industry from the perspective of actor–network theory. Telecommunications Policy. 2016 Mar 1;40(2-3):168-81.
40. Alt R, Beck R, Smits MT. FinTech and the transformation of the financial industry. Electronic markets. 2018 Aug;28:235-43.