International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| Volume 2, Issue 2, 31-35, 2021
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V2I2P104

Original Article

Dynamic Frameworks for Enhancing Security in Digital Payment Systems

Raghavendra Sridhar[1], Rashi Nimesh Kumar Dhenia[2], Ishva Jitendrakumar Kanani[3]
[1,2,3]Independent Researcher, USA.

***Abstract** - The rapid growth of digital payment technologies has revolutionized global commerce, bringing remarkable benefits but also creating new challenges in security, usability, and regulatory compliance. This study goes beyond traditional security frameworks by addressing real-world gaps in implementation, inclusive design, readiness for quantum threats, and adapting to evolving policies. Taking a comprehensive approach, the research highlights the often-overlooked disconnect between theoretical security models and their practical deployment, particularly in markets facing infrastructure limitations. It underscores the need for human-centered authentication systems, investigates strategies to reduce insider threats, and introduces proactive security measures such as role-based access controls and Zero Trust Architecture. The paper also provides practical strategies for expanding secure digital payment systems at scale without sacrificing usability or compliance, and with an eye toward staying ahead of future technological risks. These insights are intended to help software developers, financial institutions, and policymakers create resilient, inclusive, and regulation-ready payment systems for the decade ahead.*

***Keywords** - Digital Payment Security, Human-Centered Authentication, Zero Trust Architecture, Inclusive Design, Quantum Readiness, Role-Based Access Control, Regulatory Compliance, Insider Threat Mitigation, Scalable Payment Systems.*

1. Introduction

Digital payment systems are rapidly replacing traditional money handling, making their security a global priority. The rise of mobile wallets, contactless cards, open banking APIs, and cross-border platforms has increased convenience but also introduced complex cyber risks affecting users and institutions. While past research focused on technical safeguards like encryption and multi-factor authentication, today's threats require a broader view that includes human behavior, regional differences, quantum computing risks, and inconsistent global policies. Static, compliance-driven security is no longer enough. This study aims to fill gaps in current digital payment security by offering a practical, adaptable framework. It addresses often overlooked issues such as accessible authentication, insider threats, solutions for small and medium businesses, and preparation for quantum computing. The paper also discusses integrating modern security with legacy banking systems and navigating conflicting regulations across countries. Organized into ten sections, it covers real-world deployment challenges, geographic and economic tailoring, human factors, insider threats, quantum risks, legacy system integration, cost and scalability, cross-border regulations, and concludes with a clear path forward.

2. Literature Review

2.1. Putting Security Frameworks to the Test in the Real World

2.1.1. Lessons from Live Payment Systems

Real-world performance shows that security frameworks are not one-size-fits-all. While many companies follow standards, even major providers like PayPal and Stripe face breaches due to human error, third-party weaknesses, or system complexity. Advanced solutions like Apple Pay rely on tight hardware integration that is hard to replicate, while new technologies like blockchain face their own usability and integration hurdles. This proves that a successful security framework depends not just on technology, but on continuous investment in monitoring, training, and incident readiness.

2.1.2. Measuring Performance and Responding to Incidents

To know if a security framework is truly effective, its performance must be measured with clear metrics, such as fraud detection rates and breach response times. Companies with proactive, automated monitoring systems can shut down threats almost instantly, making them far more resilient. However, many organizations lack 24/7 monitoring or clear response plans, leading to greater risk, especially for smaller businesses. Evaluating a system's real-world strength means examining both its technical tools and its operational readiness.

2.1.3. The Gap between a Perfect Plan and Messy Reality

A significant gap exists between security design on paper and its real-world application. Ideal conditions assumed in theory are often compromised by business pressures, technical limitations, and budget constraints. The most unpredictable factor is human behavior, as users often bypass security measures through weak passwords or by falling for scams. This highlights a critical truth: effective security is less about a perfect blueprint and more about embedding a culture of disciplined, consistent execution.

2.2. Designing for Diverse Markets: Moving Beyond a Western-Centric Approach

2.2.1. Security in Emerging and Low-Connectivity Economies

In many developing regions, digital payments are a necessity, not just a convenience. Users often rely on basic phones, shared devices, or SMS-based platforms, frequently with unreliable internet. Security solutions must be lightweight, resilient, and able to function offline. This means using device-based tokenization, minimal data cryptography, and offline verification. Building user trust is also crucial, requiring transparent records, accessible dispute processes, and clear notifications not just strong encryption. Ultimately, security must fit the people and environments it serves.

2.2.2. Adapting for the Underbanked and Unbanked

Over 1.4 billion adults worldwide lack access to traditional financial services, often missing standard IDs or credit histories. Digital payment systems must rethink onboarding, using alternatives like biometrics, community verification, or mobile usage data. Integration with informal networks and designing inclusive interfaces such as voice navigation and multilingual support are key. Security frameworks should allow users to start with basic services and gradually unlock more features as their digital identity grows, making security an enabler, not a barrier.

2.2.3. Localization in Regulation and Technology

Applying a single security framework globally is challenging due to diverse laws, technical standards, and cultural values. For example, while the EU prioritizes data privacy, countries like India focus on data localization. Payment systems must be adaptable and modular to meet these varying requirements. Technical integration with local banks and government systems can be complex, requiring robust and flexible design. Success also depends on building local partnerships and trust. Ultimately, embracing diversity in infrastructure, regulation, and culture is essential for building secure, inclusive global payment systems.

2.3. Human Factors and Accessibility in Payment Security

The human element is critical in payment security, yet often overlooked. While technical safeguards like encryption and multi-factor authentication are essential, their effectiveness depends on how easily and reliably users can interact with them. If security features are confusing or cumbersome, users may avoid or bypass them, weakening overall protection. As payment systems become more advanced, it is vital to design security that is robust, accessible, and user-friendly for people of all ages and abilities.

2.3.1. Usability Challenges in Multi-Factor and Biometric Authentication

Multi-factor authentication is a powerful defense against fraud but can be inconvenient for users. Remembering complex passwords, carrying extra devices, or dealing with unreliable biometrics can frustrate people, especially if technology fails or is inconsistent across platforms. Privacy concerns with biometrics and inconsistent user experiences can erode trust and lead to users abandoning secure practices.

2.3.2. Inclusive Security for Vulnerable Users

Secure payment systems must work for everyone, including the elderly, disabled, and digitally inexperienced. Older adults may struggle with small screens or new authentication methods, while people with disabilities may face barriers using standard security features. Those with low digital literacy are especially vulnerable to scams. To be truly inclusive, payment systems should offer alternative authentication options, support assistive technologies, and provide multilingual, context-sensitive help. Otherwise, financial exclusion will persist—not from lack of need, but from poor design.

2.3.3. Balancing User Experience and Security

A major challenge is ensuring strong security without disrupting the user experience. Users want fast, seamless payments, but strict security measures can slow things down or cause frustration. Adaptive authentication, which adjusts security requirements based on risk, can help strike the right balance. Using AI and behavioral analytics, systems can streamline low-risk transactions and add extra checks only when needed. Clear communication and giving users choices in how they verify their identity also build trust and encourage safe behavior, making payment systems both secure and inclusive.

2.4. Insider Threats and Internal Security Risks

Insider threats, risks from employees, contractors, or vendors with legitimate access, are a major but often overlooked danger in digital payments. These insiders can intentionally or accidentally cause significant financial and reputational harm, making it essential for organizations to go beyond defending against only external attacks. Effective protection requires a layered approach that combines strict access controls, ongoing behavior monitoring, and careful management of third party relationships.

2.4.1. Role Based Access Control and Least Privilege

A strong defense against insider threats starts with role based access control and the principle of least privilege. This means giving users only the access they need for their specific job and nothing more. Sensitive tasks, like transferring funds or accessing card data, should be tightly restricted and fully logged. Regular audits are needed to prevent privilege creep as roles change. Modern identity management tools can automate these controls and ensure every privileged action is traceable.

2.4.2. Behavioral Monitoring and Threat Detection

Access controls alone are not enough. Organizations must also use behavioral analytics to spot unusual activity, such as logins from unexpected locations or attempts to access data outside a user's normal pattern. These systems use machine learning to flag potential threats and can trigger automatic responses, like revoking access or alerting security teams. Integrating these tools with central monitoring platforms ensures rapid detection and response to insider risks.

2.4.3. Managing Third Party and Vendor Risks

Most payment systems depend on a network of vendors, which increases internal risk. Effective third party risk management starts with thorough vetting, clear contracts, and tightly controlled, monitored access. Technologies like Zero Trust restrict vendors to only the systems they need. Regular assessments and integration of vendor activity into security monitoring help detect and respond to suspicious behavior. By extending security practices to all partners, organizations can build a more resilient payment ecosystem.

3. Methodology

3.1. Preparing for the Quantum Threat Landscape

Quantum computing promises revolutionary advances but poses severe risks to digital security, especially for payment systems. Current encryption methods like RSA and ECC critical for securing transactions—are vulnerable to quantum attacks. As global finance relies increasingly on digital transactions, preparing for this future is urgent for developers, fintech experts, and regulators.

3.1.1. Timeline and Post-Quantum Risks

Though large-scale quantum computers capable of breaking encryption don't yet exist, they may emerge within 10–20 years. The National Institute of Standards and Technology is standardizing quantum-resistant cryptography. Meanwhile, attackers use "harvest now, decrypt later" tactics: stealing encrypted data today to decrypt later with quantum power. This jeopardizes financial data currently considered secure, demanding long-term confidentiality planning and updated security frameworks.

3.1.2. Quantum-Safe Encryption Algorithms

New quantum-safe algorithms (e.g., lattice-based CRYSTALS-Kyber and CRYSTALS-Dilithium, hash-based SPHINCS) resist quantum attacks using novel mathematical principles. However, they aren't simple replacements their larger key sizes and structures require redesigning payment APIs, wallets, and validation systems. Careful evaluation of maturity and performance is essential before adoption.

3.1.3. Migration Roadmap

Transitioning requires a phased, dual-stack approach: supporting classical and quantum-safe algorithms simultaneously. Start with a crypto inventory audit, then prioritize critical systems like authentication servers and payment gateways. Use hybrid models for redundancy during migration. Policy updates, regulatory collaboration, and industry-wide testing frameworks ensure secure, reliable quantum-ready payment platforms. Open-source tools accelerate this transition.

3.2. Modernizing Legacy Infrastructure with Next-Generation Security

3.2.1. Compatibility Challenges in Hybrid Environments

Financial institutions operating in hybrid environments face significant security challenges when blending legacy systems with modern cloud services. Traditional platforms were not designed for today's APIs and microservices, making it difficult to enforce consistent security and authentication. These legacy systems often have outdated security, creating vulnerabilities that can compromise the entire infrastructure. Poor visibility and weak integration points further complicate security monitoring and incident response, requiring clear standards and uniform policies to bridge the gap.

3.2.2. Strategies for Migrating Legacy Systems

Transitioning from legacy systems to modern platforms is a strategic necessity for improved security and compliance. A successful migration begins with a thorough assessment, followed by a phased or modular approach to gradually update functions while minimizing disruption. This can involve using new microservices to slowly replace older components. Throughout the process, data security must be paramount, with strong encryption and auditing. This complex transformation requires close collaboration across security, development, and business teams.

3.2.3. Middleware for Secure Integration

Middleware is essential for securely connecting legacy systems to modern platforms. It does more than just facilitate communication; it enforces security policies, manages access, and monitors data flows in real time. Tools like API gateways can standardize communication and prevent attacks. By implementing a robust middleware layer, institutions can strengthen their overall security posture and innovate confidently, preserving the functionality of older systems while integrating new technologies safely.

3.3. Balancing Cost, Scalability, and Practical Adoption

Adopting robust security for digital payments requires a careful balance between operational costs and scalability. While advanced technologies offer superior protection, their financial and technical demands can be a major hurdle, especially for small and medium sized enterprises (SMEs). This section explores the financial side of security, offers tailored models for different organizations, and shows how modern technology can make security more affordable.

3.3.1. The Financial Case for Advanced Security

Implementing strong payment security involves a significant financial investment. This includes costs for advanced tools, expert staff, and continuous monitoring. However, these expenses are small compared to the devastating financial and reputational damage of a single data breach or fraud incident. The cost of a breach, including regulatory fines and customer loss, can be catastrophic. Investing proactively in security is not just a defense mechanism; it is a critical business strategy for survival and trust.

3.3.2. Tailored Frameworks for Different Business Sizes

Security is not a one size fits all solution. Large institutions can afford comprehensive, layered defenses with dedicated security teams. In contrast, small and medium sized enterprises operate with tighter budgets and fewer resources, making enterprise grade solutions impractical. Therefore, effective security frameworks must be flexible. SMEs can thrive by using modular, lightweight solutions like managed security services and open source tools, while larger organizations can implement more complex architectures like Zero Trust. This adaptability ensures security is aligned with an organization's scale and risk.

3.3.3. Automation and Cloud Security as Cost Savers

Automation and cloud native security offer powerful ways to make robust security more affordable and manageable. Automation reduces the need for manual oversight by streamlining tasks like threat detection and compliance checks, which minimizes human error and speeds up response times. Similarly, cloud platforms provide access to powerful security tools like firewalls and key management systems as a scalable, pay as you go service. This eliminates the need for expensive on premise hardware and allows businesses of all sizes to build secure, modern payment systems without breaking the bank.

4. Conclusion

This study reveals a simple truth: security on paper is not enough. The real world of digital payments is a dynamic and demanding environment, and there is a significant gap between theoretical security models and their practical, large scale implementation. To be effective, security frameworks must be proven in action, adaptable under pressure, and designed to work without frustrating users. A central theme of our findings is the need for human centered security. Technology like multi factor authentication is vital, but it must be inclusive and accessible to everyone, including elderly, disabled, or less digitally skilled individuals. Beyond usability, we identified three critical frontiers for immediate action. First, organizations must look inward and defend against insider threats using stronger access controls and Zero Trust principles. Second, the coming era of quantum computing requires proactive planning today to protect the financial data of tomorrow. Finally, the challenge of modernizing outdated legacy banking systems must be met with a gradual and layered migration strategy, using secure middleware to bridge the gap between old and new.

5. Recommendations

Looking ahead, the future of secure payments will require continuous innovation across technology, policy, and human experience. Key research areas for the next decade include developing smarter, more transparent artificial intelligence for fraud detection and making the transition to quantum resistant cryptography a reality. Further exploration of privacy enhancing technologies, like zero knowledge proofs, will be essential for building trust in an increasingly open financial world. We must also design systems that can automatically adapt to the complex and shifting landscape of global regulations. Finally, and perhaps most importantly, we must continue to put people first. Future research should focus on making security intuitive, respectful, and seamlessly integrated into the user experience, ensuring that digital finance is safe and accessible for all.

References

[1] Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28, 656–715.

[2] Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

[3] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.

[4] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612–613.

[5] Chaum, D. (1983). Blind signatures for untraceable payments. In Advances in Cryptology — CRYPTO '82 (pp. 199–203). Springer.

[6] Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. Journal of Computer and System Sciences, 28(2), 270–299.

[7] Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother obsolete. Communications of the ACM, 28(10), 1030–1044.

[8] Bellare, M., & Rogaway, P. (1994). Entity authentication and key distribution. In Advances in Cryptology — CRYPTO '93 (Lecture Notes in Computer Science, Vol. 773, pp. 232–249). Springer.

[9] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of applied cryptography. CRC Press.

[10] Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.). Wiley.

[11] Shoup, V. (1999). On formal models for secure key exchange (version 4). IBM Research Report RZ 3120.

[12] Jakobsson, M., & Wetzel, S. (2001). Security weaknesses in Bluetooth. In Topics in Cryptology — CT-RSA 2001 (Lecture Notes in Computer Science, Vol. 2020, pp. 176–191). Springer.

[13] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[14] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines (NIST Special Publication 800-63-3). National Institute of Standards and Technology.

[15] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027–2051.

[16] Kannan, P. K., & Moeinzadeh, H. M. (2019). Digital payment adoption: A review and research agenda. International Journal of Electronic Commerce, 23(3), 263–300.

[17] Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 101, 55–82.

[18] SIFMA. (2018). Insider threat best practices guide (3rd ed.). Securities Industry and Financial Markets Association. https://www.sifma.org/wp-content/uploads/2025/03/2024-SIFMA-Insider-Threat-Best-Practices-Guide-FINAL.pdf

[19] Rahman, M. A., & Lee, S. (2019). The research trend of security and privacy in digital payment. Journal of Imaging, 9(2), 32.

[20] Hassan, M. A., Shukur, Z., Hasan, M. K., & Al-Khaleefa, A. S. (2020). A review on electronic payments security. Symmetry, 12, 1344.

[21] Dhenia, R. N. K. (2020). Harnessing big data and NLP for real-time market sentiment analysis across global news and social media. International Journal of Science and Research (IJSR), 9(2), 1974–1977. https://doi.org/10.21275/MS2002135041

[22] Dhenia, R. N. K., & Kanani, I. J. (2020). Data visualization best practices: Enhancing comprehension and decision making with effective visual analytics. International Journal of Science and Research (IJSR), 9(8), 1620–1624. https://doi.org/10.21275/MS2008135218

[23] Dhenia, R. N. K. (2020). Leveraging data analytics to combat pandemics: Real-time analytics for public health response. International Journal of Science and Research (IJSR), 9(12), 1945–1947. https://doi.org/10.21275/MS2012134656

[24] Kanani, I. J. (2020). Security misconfigurations in cloud-native web applications. International Journal of Science and Research (IJSR), 9(12), 1935–1938. https://doi.org/10.21275/MS2012131513

[25] Kanani, I. J. (2020). Securing data in motion and at rest: A cryptographic framework for cloud security. International Journal of Science and Research (IJSR), 9(2), 1965–1968. https://doi.org/10.21275/MS2002133823

[26] Kanani, I. J., & Sridhar, R. (2020). Cloud-native security: Securing serverless architectures. International Journal of Science and Research (IJSR), 9(8), 1612–1615. https://doi.org/10.21275/MS2008134043

[27] Sridhar, R. (2020). Leveraging open-source reuse: Implications for software maintenance. International Journal of Science and Research (IJSR), 9(2), 1969–1973. https://doi.org/10.21275/MS2002134347

[28] Sridhar, R. (2020). Preserving architectural integrity: Addressing the erosion of software design. International Journal of Science and Research (IJSR), 9(12), 1939–1944. https://doi.org/10.21275/MS2012134218

[29] Sridhar, R., & Dhenia, R. N. K. (2020). An analytical study of NoSQL database systems for big data applications. International Journal of Science and Research (IJSR), 9(8), 1616–1619. https://doi.org/10.21275/MS2008134522

[30] McKinsey & Company. (2020, November 25). US digital payments: Achieving the next phase of consumer engagement. https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/us-digital-payments-achieving-the-next-phase-of-consumer-engagement

[31] Comerica. (2020, September 9). Digital payment security risks and best practices. https://www.comerica.com/insights/business-finance/digital-payment-security-risks-and-best-practices.html