

Cybersecurity Challenges in Mobile Payment Apps: Threats and Solutions

Salman-ul-Haq¹

¹Student, Cyber Security Management, The University of Law, Business School, Birmingham

Abstract

The study examines the evolving threat landscape, critically evaluates the effectiveness of existing security measures, and explores the complex influence of regulatory frameworks and user behaviour. Using systematic literature review methodology guided by PRISMA standards and Quality Assessment Criteria (QAS), the research synthesizes insights from a wide range of academic and industry sources. Results show that the cybersecurity landscape is changing faster than ever, with threats becoming more advanced through the use of artificial intelligence and the growing potential risks posed by quantum computing. Although technologies like encryption, tokenization, biometrics, and multi-factor authentication are available, they are often applied inconsistently, which reduces their overall effectiveness. At the same time, regulations, which are crucial, are unevenly applied across different geographies and produce inconsistencies and gaps in security measures around the globe. Human behaviours remain one of the most significant vulnerabilities, reflecting the continuing disparity between cyber safety awareness and the resultant behaviours that are truly safe and secure. The report proposes a whole systems approach that includes a range of defensive layers to provide better mobile payment security, while also developing technology, proposing a shared regulated environment globally, and recommending clear education and user-friendly design. Lastly, the report offers practical considerations for action going forward to facilitate better collaboration and partnership among developers, financial institutions, and regulators, to create a more secure, resilient and trusted digital financial system.

Keywords: Mobile Payment Security; Cybersecurity Threats; Fraud Detection; User Behaviour; Regulatory Compliance

Introduction

The emergence and globalization of mobile payments applications- including mobile or phone wallets, peer-to-peer transfer applications, and contactless payments- have changed the global financial services movement. The existence of mobile money is one of the most disruptive innovations in modern financial services, enabling users to make safe and quick transactions using their smartphones or other compatible mobile devices. As a result, cash-based financial transactions and patronage of traditional banking institutions have both experienced a drop. In recent years, it has been estimated that over 1.6 billion consumers around the world today use some type of mobile money. It is anticipated that total mobile payment revenues will reach \$12.06 trillion by 2027, and that there will be over 7.7 billion smartphone users by 2028 (Javaheri et al., 2024). This level of rapid growth is unprecedented and has occurred in part due to the widespread adoption of smartphones, the

growth of digital identity verification systems, and consumers' preferences toward contactless and convenient payment experiences (Mustapha et al, 2023).

This rapid digital progress has also increased exposure to relevant cybersecurity risks. Mobile payment platforms are the target of increasingly advanced cyberattacks which exploit vulnerabilities within the applications, the behaviour of users, and differing regulatory environments. Various vulnerabilities in technology including unsafe application programming.

Interfaces (APIs), weak encryption mechanisms, and reliance on a conglomerate of weakly vetted third-party applications--complicit with errant user and employee behaviour and mismatched risk perceptions contribute to a unique elevated exposure threat surface. Compounding matters is that in the broader regulatory environment, many jurisdictions are mismatched with data protection law, enforcement capability, or compliance laws (Frank & Kohn, 2023; Javaheri et al., 2024). The vulnerability is now multidimensional, and mobile payment security alone will never be provided by technological defenses alone; a wholly integrated response must be taken to manage all three dimensions of technology, behaviour, and regulation.

Consequently, this study was conducted with the main research question: What security threats are mainly posed by the usage of mobile payment applications, and what could be through technology, regulations, and user behavioural approaches that are enough to reduce them? To provide an answer to this question, the study will accomplish various sub-goals: identify the prevalent types of malware and cyberattacks targeted at mobile payment services; evaluate the security mechanisms such as multi-factor authentication, encryption, biometrics, and tokenization in terms of their effectiveness; analyze the influencing role of international standards like PCI DSS and the revised PSD2 in the security practice; and finally, come up with an integrated outlined model of AI- Assisted Threat Detection alongside providing the existing security frameworks for mobile payments.

The importance of this study is that it seeks to go beyond the predominant technology-focused discussion in cybersecurity to integrate behavioural and regulatory perspectives into one cohesive framework. Theoretically, it contributes to an important gap in the literature by bridging three connected pillars in the context of mobile payment security technological, human factors, and governance. Practically, it provides advice for fintech developers, financial institutions, and policy makers, seeking to address resilience and regulatory compliance across multiple regulatory environments. Socially, it highlights user education and user awareness as part of a cyber security culture and briefly justifies participative protective models and agents, which are defined as enabling users to make better decisions in a digital environment.

By engaging with issues at a global and multidisciplinary scale, this research adds to the wider challenge of building secure and trusted digital financial ecosystems. The research declares that the success of mobile payment innovation, will depend primarily on three

pillars - if financial innovation is to be sustainable, technology needs to continue to improve, regulation - needs to be innovative and harmonized, and user behaviour, will need to be educated behaviour, and continue to grow and change in line with emerging topical issues including artificial intelligence attacks, and vulnerabilities of the quantum era. This study, offered in an integrative approach, aims to contribute to both scholarly studies, and practical applications, for mobile payment system protection.

Literature Review

Defining Mobile Payment Cybersecurity

Mobile payment apps that are also referred to as mobile wallets allow people to do financial transactions, such as transfer money, pay bills, and conduct point-of-sale (POS) transactions, on their smart phones and connected devices. These apps lessen the need to use cash and visit a traditional bank. Cybersecurity in mobile payment applications involves various applications, protocols, and regulations do not allow fraud, unauthorized access to information, information leakage, and malicious software to infiltrate online transactions. The National Institute of Standards and Technology (NIST) presents a comprehensive understanding of cybersecurity, which is rooted in the complete protection of the CIA triad of digital services and comprises the perils to information systems and networks (National Institute of Standards and Technology [NIST], 2024).

Mobile payment systems are used for sensitive information such as personal identity, payment credentials, and comprehensive transaction history, therefore security measures become important. Different security techniques like encrypted data, tokenization, biometric authentication, and secure communication protocols are some of the most frequent methods applied in mobile payment applications for security (Javaheri et al., 2024).

Global Landscape of Mobile Payment Security

The global landscape regarding the use of mobile payments applications shows great regional variations. Quasi-countries like China and India most extensively rely on QR codes due to the extensive existing infrastructure of QR code acceptance and state sponsored programs encouraging the use of mobile payments. In contrast, sophisticated technological nations, such as the USA and UK, make use of mobile platforms like Apple Pay and Google Pay, which are already a part of the traditional banking system and likewise applying strong biometrics features. Other adoption models are present in Africa like M-Pesa which have been playing a vital role in providing financial services to the remote areas where the traditional banks are not present (Javaheri et al., 2024).

Security is a major problem that comes with the wide usage and penetration in these different global contexts The Global Banking Crime Survey showed a considerable rise in electronic crimes and cited the growing trust in mobile payments as one of the main reasons. Although the existing platforms provide the best security/ protection measures available nowadays (e.g., fingerprint scanning, tokenization, and data encryption), there remains a

substantial gap between the processes of domestic and international standardization. Non-standardization results in certain areas having lesser security, particularly when either the regulations are not strictly followed or the network structure is not properly developed (Javaheri et al., 2024).

Income inequality has emerged in mobile payment security across countries, primarily influenced by varying regulatory maturity, along with heterogeneous technological infrastructure and user education. The outcome is a fragmented global security, presenting a risk of vulnerability to the global electronic financial network. As identified in the foundational document, inconsistent storage of the law and differences between jurisdictions lead to inconsistent integrity in mobile payments. It outlines challenges in developing countries such as, "Incapable infrastructure, low resident literacy levels, and absence of regulation to govern activity" (Javaheri et al., 2024). This demonstrates that security is inconsistent and utilized in different capacities through the global south leaving mobile payment security a patchwork rather than a cohesive global defense. Ultimately, global mobile payment infrastructure remains a patchwork of different levels of maturity determined by policy, legislation, infrastructure and user education. The fragmented nature of the global mobile payment infrastructure creates systemic weakness as "a chain is only as strong as its weakest link".

Prevalent and Emerging Cybersecurity Threats

The idea that mobile phones are always filled with software, linked to various third-party applications, and that users can do countless things on them, make mobile phones are appealing to protect from cyber attackers (Javaheri et al., 2024).

Phishing and social engineering attacks

They remain one of the most essential risks that mobile payments face. Criminals utilize their creativity to develop misleading messages, formulating phishing messages (via SMS), or phishing messages (using email), to deceive users into sharing sensitive information (Basit et al., 2023). Individuals who possess a lower level of cybersecurity awareness may be especially vulnerable to such attacks. Research revealed that 78% of the phishing impersonators went ahead and clicked on the links even after getting a proper warning about it (Thomopoulos et al., 2024). Generative AI has even more sophisticatedly opened up the attack frontiers by producing personalized, likeable, inviting phishing emails and fake websites that are characteristic of the attacks in terms of scale, speed and being spread globally (ISACA, 2024; Javaheri et al., 2024).

Malware and Spyware Infiltration

There is a possibility that malicious software like Trojan viruses and spyware could illegally access mobile payment applications by tricking users into installing fake apps or using infected third-party apps. These malicious programs would then monitor the user, steal their password, and perform unauthorized activities after being installed. Nevertheless, the attacks

like EventBot and Anubis that targeted banking systems are still going strong among other examples. According to the report, apps account for 70 percent of all mobile malware distribution and Android, with its open architecture, is the platform on which 95 percent of mobile malware infections occur worldwide. In 2023 alone, over 3.5 million mobile malware threats were newly detected, which serves as a clear indication of the fast-paced evolution of these attacks (Zimperium, 2024). To illustrate, the Zangis banking Trojan was born in mid-2022 and it is a timely messenger of that transformation, given its implementation of sophisticated obfuscation techniques, social engineering (that includes fake educational pages), extensive data gathering, SMS interception (to avoid two-factor authentication), and even producing a sense of trust and ownership through deception of updates. It employs the Android Accessibility Services capability to acquire escalated privileges and perform malicious acts without the user's awareness. SIM swap identity theft is a scenario wherein a criminal discovers the flaws in the mobile phone network and obtains a SIM card with the victim's number transferred on it. The attacker can then impersonate the victim and gain access to the payment apps related to the account, which he can do simply by changing the password through SMS verification code. SMS authentication has been one of the biggest contributing factors to the issue due to its inherent nearsightedness and sometimes inconsistency in telecommunications i.e. (Javaheri et al., 2024). The FBI in 2022 forecasted that SIM swapping accounted for over \$72 million in losses, which has evidently worsened the situation. The attacks that can occur via the attacker being in collusion with the system are selling or imparting knowledge from a previous security breach at the carrier's (e.g., T-Mobile, Verizon, AT&T, etc.) to CPNI (FBI, 2023).

Man-in-the-Middle (MitM) and Network-Based Attacks

The Man-in-the-Middle (MitM) attack occurs when a malicious actor listens and intercepts the communication of two parties thinking they are in direct connection. public Wi-Fi and open networks are the most common environments for such attacks (NIST, 2024; OWASP Foundation, 2024). Even if the data is encrypted, it can still be accessed by a compromised Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol (NIST, 2024). Attackers can capture authentication tokens over the Internet allowing them to impersonate online sessions and change any stored log-in data (OWASP Foundation, 2024). Lack of mutual authentication and certificate pinning creates a disadvantage for the system (OWASP Foundation, 2024). Most importantly, attacks on mobile devices are more frequent than on laptops because smartphone users are more engaged in sensitive activities (NIST, 2024; OWASP Foundation, 2024). Public Wi-Fi Networks are rated in terms of dangers, because the encryption of the communication is absent, hence, it can be intercepted; besides, fake Wi-Fi networks can lure users into revealing their credentials.

Weak APIs and Integration Weaknesses

Mobile payment systems that use APIs carried the necessity of having a communication layer among user interfaces, databases, and the connected noted systems. In contrast, insecure APIs provide a plethora of chances for an attacker to intrude. Misconfigured ports

and related protocols, unsecured data traffic, lack of security measures, or unprotected data can all be the sources of vulnerabilities (Javaheri et al., 2024). There exist many mobile applications that still do not provide a secure runtime and hence can be easily exploited through the APIs in application packages or executables. Among the most common security gaps for APIs are these weaknesses: Open Object Level Authorization (BOLA); Broken Authentication; Unnecessary Data Exposure; No Rate Limiting; Injection flaws; Improper Assets Management; Insufficient Logging & Monitoring; Insecure Direct Object References (IDOR); and use of components with known vulnerabilities (OWASP Foundation, 2024).

Data Breaches and Privacy Violations

Mobile payment applications have to deal with the management and storage of large amounts of personal and financial data, which are sought after by hackers and targets for data breaches (Javaheri et al., 2024). Poor in-house regulations are believed to be one of the leading causes of data breaches and misconfigured databases in the organizations is another cause. If companies do not comply with regulations such as GDPR and CCPA, which are all about data privacy, the situation becomes serious from both legal and economic points of view (ENISA, 2024). As a case in point, there was an improper configuration of a database that resulted in the unintended leakage of real-time order data of millions of customers together with even more sensitive information such as phone numbers, delivery notes, and credit card data. The clients are concerned about the handling of their personal data and, therefore, they expect that their financial applications should be accountable and efficient in privacy (ResearchGate, 2025u).

Emerging Threats: AI-Powered Attacks and Quantum Risks

Attacks Powered by AI

One of the digital dilemmas faced by the security industry is the rising number of attempts where the malicious attackers have been using Artificial Intelligence to get better in automating and enhancing the effectiveness of their evil activities. Among these attempts are impersonating user actions, devising highly deceptive communications that are potentially undiscriminated, and creating dynamic viruses (Dwivedi et al., 2023; ISACA, 2024). Adversarial AI attacks are associated with the clever but nefarious idea of subtly modifying the input data, tricking the Machine Learning (ML) model into misclassifying or incurring a possible wrongful initiation of behaviour (usually in fraud alert systems) (Kong et al., 2021).

Quantum Risks

The development of quantum computing has its dark side as the technology that has opened the door for performing unimaginable tasks also poses the risk of modern encryption being broken (Javaheri et al., 2024). A great case in point is the Shor algorithm which besides easily cracking the RSA method of encryption via integer factorization also threatens ECC, i.e., the algorithm based on discrete logarithm which compromises the long-lasting use case

of being implemented as a cryptographic algorithm. In comparison between asymmetric cryptography and symmetric (EX: AES, SHA-256), the latter is more at risk due to the Grover algorithm, which reduces the brute-force search space. According to the predictions made by industry analysts, especially Gartner, quantum computing will start threatening traditional cryptography by the year 2029 at the earliest. Indeed, the increasing complexity of cyber difficulties could be blamed directly on the skilled and talented criminals who, among others, are using the latest technologies, such as artificial intelligence and quantum computing, and taking advantage of the existing weaknesses consisting of humans making mistakes, lack of regulations, and poorly secured networks, which are all done unsuspectingly. This creates a situation where the security has to constantly adapt to the attackers' innovations. One of the trends stated in the founding document is that "the situation has changed in such a way that today security measures are more likely than ever to respond to threats rather than prevent them" or something along these lines. Numerous reports indicate that attackers, for instance, are employing AI to generate realistic phishing attacks (ISACA, 2024; Javaheri et al., 2024), create new and constantly changing malware (ISACA, 2024), and even some authors include AI in the process of tricking fraud detection systems (Motie & Raahemi, 2024). Quantum computing is one of the technologies that pose substantial risk as it is projected to be a source for developing new (threatening to the current) encryptions. At the same time, the human aspects are pointed out as the reasons for the problem, for example, "low literacy" and "user behaviour" along-side "regulatory inconsistencies" (Javaheri et al., 2024). This interconnected organization signals that there is a strong trend: the better the defenses become on the tech front, the more offensive defenses are growing simultaneously using new technologies and capturing the weaknesses of the system to exploit which commonly takes place outside the tech sphere (the best targets are often the implementation gaps).

Existing security measures and their performance

Gradually mobile payment solutions have adopted various security Control Technology Layers (CTLs) in their efforts to protect the confidentiality of financial data, verify the user's identity or secure the transaction. Nevertheless, the actual performance of those tools depends on their unified software application, users' secure behaviour and compliance with a regulatory framework (Frank & Kohn, 2023). Encryption and Tokenization: The main source of mobile payment security is through encryption - specifically, End-to-End Encryption (E2EE) and Transport Layer Security (TLS). The basic assumption of encryption is that an unauthorized third-party will not be able to comprehend the message even if it is intercepted. Tokenization is yet another key process that substitutes sensitive card data with unique, randomly generated tokens and lessens the worth of the stolen data for the possible fraudster who does not have access to (or can't reproduce) the original transaction (Javaheri et al., 2024). As per a related study, network tokenization offered several advantages and will curtail fraud along with boosting transaction approval rate by more than 2.2% while cutting fraud by 26%. PCI DSS requires cardholder data to be encrypted both during storage and

transmission and has specified a list of encryption algorithms that are considered acceptable which include AES, RSA, TDES/TDEA, DSA/ D-H, and ECC (PCI Security Standards Council, 2022). The presence of these benefits also brings about the problem of possibly unequal adoption or simply ignoring the secure data storage options (Javaheri et al., 2024).

Biometric Authentication

The full range of biometrics (fingerprints, facial recognition, and iris scanning for instance) is being employed extensively due to the security and the user-friendliness aspects (Jain et al., 2011; Marasco et al., 2023). The international market of biometric systems, which is counted to exceed 82.9 billion dollars, indicates their high acceptance by the consumers. Financial institutions worldwide have recognized the biometric authentication systems they account for approximately 64 percent of the total use. Besides, certifications from 85 percent of banking customers believe that they are tech-savvy enough to cope with biometric processing and 92 percent who find it more convenient than conventional passwords. The Bank of America mobile app case demonstrated the impact of biometric security as it had a fraud decrease by 52 percent (Jain et al., 2011). Using top-notch machine learning algorithms, the accuracy rate of facial recognition can be pushed up to 99.97 percent and "liveness" measurements can be taken to prevent spoofing attacks (Pratama et al., 2025). Iris recognition has been recognized for its high security, durability, reliability, and real-time identification along with being age-invariant and having a low accuracy error rate. Moreover, it is claimed that iris scanning can be done even through most smartphone cameras. Still, some researchers bring up the issues of the necessity to have biometric data as a backup or the protection of non-modifiable identifiers (NIST, 2024) (see figure 1).

Technology Effectiveness (0–100)

Encryption & Tokenization

90%

Biometric Authentication

85%

Multi-Factor Authentication (MFA)

80%

Blockchain

65%

AI/ML-based Detection

75%

Figure 1. *Technology Effectiveness*

Technological Enhancements in Mobile Payment Security

Multi-Factor Authentication (MFA)

MFA makes mobile payments transactions more secure since the user has to verify himself using two different factors, and these are: knowledge, possession or inherence, and there is no room for DDoS and phishing attacks. Then, adaptive MFA takes the user experience to a whole new level since it will be able to adjust the requirements based on the user's context thereby lessening the burden on a user and preventing user fatigue with MFA (NIST, 2023). In spite of that, there are still weaknesses such as SIM swapping, social engineering, adversary-in-the-middle (AiTM) attacks, and others that are especially pertinent to the use of OTP for SMS authentication (OWASP Foundation, 2024; Strata.io, 2025).

Blockchain Integration

Blockchain technology entails a reliable networking solution that potentially improves the security of mobile transactions. Blockchain is a decentralized, transparent record-keeping technology, and when configured with protocol rules, blockchain can identify the confirmation of identification elements in permissioned smart contracts (Hafez et al., 2025). This technology enables users to make secure payments across international boundaries, protects against fraud, and offers improved tracking (Casino et al., 2019; Rattanawiboonsom & Khan, 2024; Hafez et al., 2025). Challenges such as scalability issues, costs of integration, legal ambiguity, and lack of harmony among various regulations constrain functionality in the mainstream (Hafez et al., 2025).

Artificial intelligence and machine learning (AI / ML)

Artificial Intelligence (AI) and Machine Learning (ML) are additional technologies used in mobile payment systems to monitor fraud and flag anomalies in-measured, or near-real time, through transaction history and or user behaviour analysis (Btoush et al., 2023; Vijayanand & Smrithy, 2025). The approach is either supervised learning (neural networks) or unsupervised approaches (K-means, Isolation Forest) to achieve detection with a reasonable degree of accuracy and low incidence of false positives. Experts and researchers have also noted in regards to the ethics of using AI, there are problems with the algorithm, including biases in decision making and transparency (Adil, 2025). As a result, there has been a growing interest in Explainable AI (XAI), defined as a set of methods and approaches to provide transparency (Weber et al., 2024).

Secure App Development Practices

Security-by-design has increasingly been adopted in Mobile payment applications to their apps together with best practice (secure coding, API protection, run time security (e.g., RASP), platform-native protocols (e.g., SafetyNet, Secure Enclave) adherence.

Nevertheless, the application of Owasp Mobile Top 10 recommendations by the developers

is not sufficiently leading to vulnerability, since the insecure storage and insecure communication methods are some of the most serious attacks leaving the systems open (OWASP Foundation, 2024). Thus, security should be an integral part of all Mobile App Development Lifecycle (MADLC) activities (OWASP Foundation, 2024).

Regulatory Frameworks and Compliance

Mobile payment security vulnerabilities are influenced by new regulatory policies including Payment Services Directive 2 (PSD2), PCI DSS, and GDPR. PCI DSS disclosure obligations entail strict criteria requirements that specify that service providers use tokenization, encrypt cardholder data. For PSD2, the EU requires customer authentication to have a high assurance level, but this level of authentication is not implemented on a worldwide basis (Romănova et al. 2018). Data privacy laws like GDPR and CCPA create obligations that prohibit any contingencies and force consumers to provide clear consent to process the data (ENISA, 2024). Reasons for this variation include not every country has successfully implemented the regulations or developed countries with issues in socio-economic development, legal means of enforcing laws, educational needs or even infrastructure to enforce regulations. The global defragmentation in the regulatory process diminishes the overall global cybersecurity resilience a single regulation would provide because it creates multiple opportunities for a criminal to access the data, and policing does not ensure adequate security or protection of the consumer (Javaheri et al., 2024). It is practically impossible to have a global harmonized regulation system or to practically create an agreement to conform all mobile payments to a single international regulatory scheme (see figure 2).

Global Mobile Payment Regulatory Maturity

Region	Key Regulation	Maturity Level
Europe	PSD2, GDPR	High
United States	CCPA, PCI DSS	Medium
Africa	National Data Policies	Low
South Asia	Patchwork Guidelines	Low
China	Cybersecurity Law	Medium

Figure 2. *Global Mobile Payment Maturity*

Global regulatory harmonization is still quite unrealistic owing to various structural barriers. Each nation keeps its exclusive power over financial regulation, thus making it impossible to apply universal standards. There are also striking differences between the countries regarding economic capacity, technological development, digital literacy, and the capability of the institutions to enforce the law. Developing countries are usually the ones who lack the necessary resources and the infrastructure to either adopt or enforce the very complicated cybersecurity laws, while the developed nations are operating in a legal framework that is compatible with none but matured. Moreover, there are differences in policy priorities, rivalries in geopolitics and different interpretations of data sovereignty which have the effect of further reducing the likelihood of a global regulatory system that is unified and seamless.

As a result, full harmonization of global mobile payment regulation is still a matter of politics and operationally unattainable.

Considering these limitations, the use of practical interim frameworks will be the most interoperability methods to be adopted for global cybersecurity alignment. Different countries might set minimum requirements that may differ from one another but will still be in the same line, such as ISO/IEC 27001, PCI DSS, and NIST guidelines that are not the same but will be helping in making the same law indirectly. The European Union, ASEAN, African Union, or similar unions can also serve as a regulator through which different regions with similar cultural and economic backgrounds will be aligned. To prevent inconsistencies during cross-border transactions, mutual recognition agreements among countries can be implemented wherein compliance in one area will be recognized by another. In addition, voluntary certification programs and industry standards will provide a trusting yet unified atmosphere for mobile payment providers worldwide. Thus, these stepwise methods are the ones that together represent realistic ways of making the world more coherent in terms of regulations without the need for full regulatory unity at the same time.

Influence of User Behaviour on Security Adoption

Consumer practices continue to be a primary determinant in the security of mobile payments, while on the other hand, consumer behaviour, still affecting the security side negatively, albeit with a good deal of knowledge, is demonstrated through such things as the use of weak passwords, turning off MFA, etc., which are considered insecure, mainly because of the choice of low digital literacy, misleading user interfaces and convenience versus security preferences. The use of visual stimuli along with the layout of the interfaces is crucial in the process of winning user trust and acceptance of the security measures; at the same time, the proper behavioural use is further enhanced by the presence of noticeable signs of security (Behera & Kumra, 2024).

Lack of knowledge, especially, does not play a major role in the acceptance of security mitigations; on the contrary, it is determined by the context and psychological factors that are connected to the perceptions of threat relevance and usability (Arlı, 2023). Therefore, it is not possible to build long-term user engagement and compliance to security measures based on trust that is fostered through transparent intuitive design. Eventually, the most sophisticated technologies and the strongest policies are still effective only if they cause active user participation and alignment of behaviour (Behera & Kumra, 2024).

The accumulation of literature examined suggests that mobile payment security is not just a technology-dependent area but one where human and regulatory aspects need to be integrated as well.

Methodology

Research Design

This research employs a Systematic Literature Review (SLR) to study cybersecurity risk

within mobile payment systems, during a time when mobile transactions have become prevalent, ensuring adequate digital security. This methodology has a structured, transparent, and reproducible method for identifying, evaluating, and synthesizing previous research to build evidence-based knowledge, which is applicable to both policy and practice.

Research Method

The SLR method was chosen for its ability to systematically aggregate interdisciplinary evidence related to technology, regulation, and human behaviour. This research takes a positivist research paradigm by using data that can be measured and observed to reach credible conclusions. The SLR review was overall performed, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines and with a Quality Assessment Criteria (QAC) to validate and establish rigor of the studies that were included and reviewed.

PRISMA Framework

The PRISMA framework organizes the review process into a transparent and replicable process of four stages: identification, screening, eligibility, and included studies. A PRISMA flow diagram provides visibility along the process of studies that justify inclusion or exclusion in the review process.

Quality Assessment Criteria

The quality assessment criteria (QAC) is used to evaluate methodological transparency, relevance to the research aims, strength of evidence, and the value of journals in publishing reporting. Only high-quality and peer-reviewed articles meeting these criteria were included in the review process, the reviewed studies provided maximum reliability when synthesizing findings.

Search Strategy and Data Collection

To have access to a variety of scientific papers related to the security of mobile payments, a search strategy that was systematic and reproducible was developed by us. The searches that we did were in the most important and relevant academic databases which are IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Scopus, Web of Science and Google Scholar. We made use of Boolean logic and the search terms that were created (for instance, "Mobile Payment" AND "Cybersecurity Threats" or "Blockchain" AND "Mobile Payment Security"). The syntax was adjusted according to the specific database.

Inclusion criteria

Only peer-reviewed articles, conference papers, technical reports, and government publications from 2014-2024 that met a strict three-step relevance search framework were included. Non-academic materials including blogs and news articles were excluded. Also excluded were studies that did not concern technology, law, or human-behaviour studies.

Data Management

Employing a structured spreadsheet, we recorded all studies identified, along with their bibliographic information, abstracts, relevance ratings, and eligibility notes. This transparency ensured both traceability and reproducibility of the multisource literature review process, graphically summarized by the PRISMA flow diagram.

Data analysis

Data analysis was undertaken using a thematic synthesis approach, whereby data were extracted and coded into categories that represented the main themes of the research, such as, types of cybersecurity threats, security mechanisms, regulatory influence, and user behaviour. Thematic replication, inconsistencies, and gaps in research were identified through cross-comparison of the findings. The QAC was employed to evaluate the methodological quality of each study included, thus ensuring the synthesized conclusions have enough trustworthiness and dependability.

Findings and Discussion

Synthesis of Key Findings

The systematic review of the literature indicates that mobile payment security represents a multi-faceted concern that has emerged and developed due to the rapid evolution of cyber threats; inconsistent use of security technologies; fragmented and inconsistent regulatory regimes around the globe; and the increasing role of user behaviour and technology acceptance. Collectively, these implications confirm that technological safeguards alone will not guarantee security. Instead, trusted protection for mobile payment systems will require a harmonized approach to security that incorporates human behaviour, organizational approaches, and regulatory responses in a holistic manner.

Discussion of Threat Evolution and Implications

As mobile payment adoption continues to expand, and cyber attackers become increasingly adept at circumventing established security protocols, it is clear that cyber attackers are now able to exploit artificial intelligence (AI), and other emerging quantum computing capabilities, to develop adaptive and stealthy attacks. Notable advances in AI-enabled phishing, polymorphic malware, and adversarial manipulation of fraud detection systems underscore the limitations of traditional reactive security models to confront mobile payment security (ISACA, 2024; Javaheri et al., 2024). Furthermore, AI-based attacks may be observed albeit quantum computing presents the more ominous long-term threat and possible attack vector wherein contemporary cryptographic algorithms RSA, ECC, and AES will be compromised to an extent that renders them useless, with some suggesting that as early as 2029 (Motie & Raahemi, 2024).

In addition to human-oriented challenges with aspects including limited capabilities in digital literacy technology, and inconsistent compliance with requisite ICT security practices around any given mobile payment transaction, regulatory obligations vary considerably by region. Case study evidence points to the impact of, and implications imparted by, these

aspects of mobile payment technology, particularly in terms of financial loss, decreasing user trust and brand reputation for established companies. The burdens that these challenges impose on product developers provides additional rationale for the need for flexible, adaptive, and holistic mobile payment security strategies.

Critical Evaluation of Security Technologies

Various security mechanisms have been employed throughout mobile payments ecosystems with varying effectiveness:

- **Encryption and Tokenization:** Having end-to-end encryption (E2EE) and Transport Layer Security (TLS) as mainstays of security mechanisms is often effective in protecting transactions while tokenization limits exposure in the event of a data breach (Javaheri et al., 2024). Often their benefits are diminished by inevitable poor implementation and configuration error (NIST, 2024).
- **Biometric Technology:** Biometric verification using AI and verification technology with “liveness” detection increased overall authentication accuracy (Marasco et al., 2023). Nevertheless, the issues of privacy infringement remain when stealing biometrics and the performance and durability of such technology (NIST, 2024).
- **Multi-Factor Authentication (MFA):** Adaptive MFA is a strong layer of protection notwithstanding vulnerabilities to SIM swapping, MFA fatigue, and Adversary in the Middle (AiTM) (OWASP Foundation, 2024).
- **Blockchain:** Provides transparency and immutability which can strengthen anti-fraud mechanisms (Hafez et al., 2025) but, its use is still curbed due to scalability, cost, and possible future regulation (Rattanawiboonsom & Khan, 2024).
- **AI and Machine Learning (ML):** Offers improvements for fraud detection and behavioural analytics, but data bias even in interpretability, and privacy issues are present (Motie & Raahemi, 2024).
- **Secure Development Practices:** Properly applied elements from OWASP best practices, along with runtime application self-protection (RASP) tools, can twice the resilience against a security breach. Still, the gradual and limited use of such tools eventually keeps the threat alive (OWASP Foundation, 2024).

Ultimately, the effectiveness of these technologies’ hinges upon ongoing application, interoperability, and appropriate governance within the larger ecosystem.

Regulatory Gaps and Global Disparities

Regulatory standards (e.g., PSD2, PCI DSS, and GDPR) are the pillars of data protection and consumer protection, but they are only here and there adopted, which again turns out to be the main reason for the reduced effectiveness. In some developing economies, regulatory support is underdeveloped or poorly enforced partly due to infrastructure issues and limited

technical expertise (Javaheri et al., 2024). In developed economies, while compliance ecosystems are overall more reasonably developed, regulatory standards related to cross-border data governance and interoperability remains challenging. Such regional disconnects results in an overall dysfunctional global regulatory framework that complicates efforts toward collective cybersecurity (ENISA, 2024).

The Human Factor: Closing the awareness-compliance gap

The human factor(s) still represents one of the most fundamental vulnerabilities in respect to mobile payment security. Users regularly undermine protections by enabling weak passwords, disabling multi-factor authentication (MFA), or being victimized by social engineering attacks (Frank & Kohn, 2023). Studies have found that awareness of potential threats does not inherently lead

to secure behaviour when compliance is driven by cognitive, cultural, and interface design (Arli, 2023; Oliveira et al., 2016). Additionally, cybersecurity responses are more often reactive than proactive, being exhibited in behaviour after an incident occurred (Yang et al., 2023). Proactivity in security area means the need for proper directions, user-friendly design, and continual digital literacy effort.

Comparative Review of Platform Security

A comparative review found significant differences in the approach to security relating to different platforms and regions:

- China (Alipay, WeChat Pay): sophisticated AI based analytics and QR code management offered strong defenses.
- Europe (Monzo; Revolut): demonstrated the ability to integrate regulation and technology with PSD2 protections, dynamic CVV coding, and preventative fraud alerts.
- Africa (M-Pesa): security social issues, infrastructure limitations and high susceptibility to SIM-swap fraud continued to undermine security efforts.
- South Asia (Paytm): Users were completely unaware of educational deficiencies and economic disparities were evident in operating system updates.

The evidence follows that security solutions must also be localized, bearing in mind technology readiness, cultural conventions, and regulatory capacity.

Synthesis of Findings and Identification of Persistent Gaps

The review draws attention to several systemic weaknesses to which mobile payment security is vulnerable:

- Threat Evolution: The risk environment is becoming increasingly complex fueled by AI-based threat options and post-quantum considerations.
- Technological Gaps: There are sophisticated tools available, but they are not being

widely deployed.

- **Regulatory Gaps:** Security is not being enforced equally, especially outside the EU and U.S. context.
- **People Dependability Issues:** Low levels of cyber awareness, poor behavioural design to protect users/humans, and poor UI design are all weaknesses.
- **Regional Issues:** Context-specific issues require different policy and technical responses.

These weaknesses result in gaps in implementation, enforcement, and user participation. The growing security gap increasingly looks like a lack of balance between the sophisticated nature of threats and the sophistication of our current defenses. The only way to bridge the growing security gaps is to build an approach that is coordinated across the whole-of-government and other involved actors including developers, regulations, and end-users, and is also built to a resilient and adaptive global security ecosystem.

Technical and Regulatory Recommendations

This study has made several recommendations both technically and in terms of policy to mobile payment security enhancement.

On the technical side, there will be the necessity of constant innovation to effectively handle the coming threats which mainly are the usage of artificial intelligence for malicious purposes and the advent of quantum computing. The financial services firms would have to go for universal user verification techniques such as multi-factor authentication, machine learning-based fraud detection systems, along with zero knowledge encryption techniques and auditing at intervals. The growing sophistication of cyberattacks has made it a necessity for governments and financial regulators to support the exchange of real-time threat intelligence across sectors along with collaboration.

From a regulator's viewpoint, the synchronization of mobile payment security standards on a global scale should be sorted out as a priority during the joint effort, through the involvement of international organizations like the World Trade Organization (WTO) and the International Monetary Fund (IMF). Besides, the introduction of the security certification for mobile payments that the third party is mandatory will not only increase the accountability of the system but also the user's confidence. Also, the laws regarding data protection should be updated to include biometric and behavioural identifiers in the category of intellectual property, guaranteeing the full protection of personal data. For the case of developing countries, the governments should rely on the telecom operators to help them in the fight against fraud based on SIM-swapping and identity theft, which would not be effective without real-time detection. Flexible and modular approaches to regulation for emerging technologies such as blockchain and AI will be necessary to tackle issues of algorithmic bias, privacy of data, and liability of smart contracts.

User-Centered Recommendations

As the human aspects of behaviour are among the most influential on the cybersecurity domain, user experience and education should be given the importance they deserve. Gamified training and educational programs in cybersecurity can replace passive awareness campaigns by providing an interactive, experiential learning experience that reinforces secure behaviours. Application interfaces should clearly indicate the status of security features, such as multi-factor verification and tokenization, to foster user understanding and trust.

The security-by-design approach should be adopted by mobile payment services, which would result in necessary protections that would be switched on by default with an option for the user to turn them off whenever they wish. Continuing, culture-aware awareness campaigns should focus on users and highlight evolving threats and protective behaviours. Efforts to simplify privacy policies and align them with global models (such as GDPR & CCPA) would enhance user interpretation, trust, and compliance regarding digital payment platforms.

Future Research Directions

Although this study offers an extensive synthesis of current challenges and solutions in cybersecurity within mobile payment systems, further studies are needed to improve empirical understanding. Future studies should empirically test the suggested frameworks in diverse cultural and regulatory contexts, using either qualitative or quantitative methods. Comparison research across sectors and regions can identify process nuance in compliance, security maturity and user behaviour. Longitudinal research is needed to assess the ongoing impact of security intervention features like adaptive multi-factor authentication and behavioural monitoring.

Ethical and transparent AI use in fraud detection should be the focal point of future research as the company will aim to eradicate bias and build up consumer trust. It has also been indicated that more studies will be needed to understand the scalability, energy consumption, and interoperability challenges related to blockchain technology. Lastly, interdisciplinary research will be important in understanding how user behaviour and compliance are impacted by cultural, socioeconomic and digital literacy issues, and to create inclusive cybersecurity strategies that are adaptable worldwide.

Conclusion

Conducted via a Systematic Literature Review (SLR), this research emphasizes the fact that mobile payment security is a multi-faceted problem, which needs to be solved by a cross-disciplinary approach, namely the cooperation of technology, legislation and user behaviour. The mobile payment ecosystem has been considerably fortified owing to technological improvements and regulatory reforms that continue to be rife with large-scale weaknesses. Weak third-party integrations, global standards lacking consistency and a general low level of user awareness are the vulnerabilities highlighted in the study. The quick rise of AI-based

attacks and the expected disruptions caused by quantum computing have added to the difficulties faced by mobile payment systems.

One of the major reasons given for the problem the study highlights is not the unavailability of sufficient technology or regulations, but the dissipation of the stakeholders. Mobile payment security needs a comprehensive framework that encompasses technology, global policy, and user. Only then will the industry get the resilience, trust, and sustainability of digital money systems that last a long time.

References

- Adil, K. (2025). Leveraging advanced data techniques in HR analytics: Revolutionizing workforce management. *Journal of Social Research Dynamics*, 1(1).
- Arli, D. (2023). Exploring the role of innovation attributes on mobile payment adoption. *Journal of Consumer Marketing*, 40(7), 826–841. <https://doi.org/10.1108/JCM-04-2021-4630>
- Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2023). Mitigation strategies against phishing attacks: A systematic literature review. *Computers & Security*, 132, 103387. <https://doi.org/10.1016/j.cose.2023.103387>
- Behera, C. K., & Kumra, R. (2024). Two decades of mobile payment research: A systematic review using the TCCM approach. *International Journal of Consumer Studies*, 48(1), e13003. <https://doi.org/10.1111/ijcs.13003>
- Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, 9, e1278. <https://doi.org/10.7717/peerj-cs.1278>
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R.,
- Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., ... Wamba, S. F. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>
- European Union Agency for Cybersecurity. (2024). *Data protection and cybersecurity in digital financial services*. <https://www.enisa.europa.eu/>
- Federal Bureau of Investigation. (2023). *Internet Crime Report 2022*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- Frank, M.-L., & Kohn, V. (2023). Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. *Computers & Security*, 132, 103386. <https://doi.org/10.1016/j.cose.2023.103386>
- Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A

- systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, 12(1), Article 6. <https://doi.org/10.1186/s40537-024-01048-8>
- ISACA. (2024). *Artificial intelligence and cybersecurity: Opportunities and threats*. ISACA Journal. <https://www.isaca.org/>
- Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 241, 122697. <https://doi.org/10.1016/j.eswa.2023.122697>
- Kong, Z., Xue, R., Wang, G., Zhai, Q., Huang, S., & Wang, C. (2021). A survey on adversarial attack in the age of artificial intelligence. *Wireless Communications and Mobile Computing*, 2021, Article 4907754. <https://doi.org/10.1155/2021/4907754>
- Marasco, E., Albanese, M., Patibandla, V. V. R., Vurity, A., & Sriram, S. S. (2023). Biometric multi-factor authentication: On the usability of the FingerPIN scheme. *Security and Privacy*, 6(1), e261. <https://doi.org/10.1002/spy2.261>
- Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, 240, 122156. <https://doi.org/10.1016/j.eswa.2023.122156>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. <https://www.nist.gov/cyberframework>
- Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and security trust. *Computers in Human Behavior*, 61, 404–414. <https://doi.org/10.1016/j.chb.2016.03.030>
- OWASP Foundation. (2024). *OWASP Mobile Top 10 Risks*. <https://owasp.org/www-project-mobile-top-10/>
- Pratama, M. H. A., Rizal, A., & Irawati, I. D. (2025). Advancing secure face recognition payment systems: A systematic literature review. *Information*, 16(7), 581. <https://doi.org/10.3390/info16070581>
- PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard (PCI DSS) Version 4.0*. <https://www.pcisecuritystandards.org/>
- Románova, I., Grima, S., & Spiteri, J. (2018). PSD2 and open banking: Regulatory implications for FinTech innovation. *Journal of Risk and Financial Management*, 11(3), 47. <https://doi.org/10.3390/jrfm11030047>
- Thomopoulos, G. A., Lyras, D. P., & Fidas, C. A. (2024). A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective. *Personal and Ubiquitous Computing*, 28, 449–470. <https://doi.org/10.1007/s00779-024-01794-9>
- Vijayanand, D., & Smrithy, G. S. (2025). Explainable AI-enhanced ensemble learning for financial fraud detection in mobile money transactions. *Intelligent Decision Technologies*, 19(1), 52–67. <https://doi.org/10.1177/18724981241289751>
- Weber, P., Carl, K. V., & Hinz, O. (2024). Applications of explainable artificial intelligence

in finance: A systematic review of finance, information systems, and computer science literature. *Management Review Quarterly*, 74, 867–907. <https://doi.org/10.1007/s11301-023-00320-0>

Yang, C.-C., Yang, S.-Y., & Chang, Y.-C. (2023). Predicting older adults' mobile payment adoption: An extended TAM model. *International Journal of Environmental Research and Public Health*, 20(2), 1391. <https://doi.org/10.3390/ijerph20021391>

Zimperium. (2024). *Global Mobile Threat Report 2024*. <https://www.zimperium.com/global-mobile-threat-report/>

© The Author(s) 2025. Published by International Association for Social Research Dynamics. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.