Anvar Sadath A K, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Securing Mobile Banking Ecosystems: An Integrated Survey of Cryptographic Standards, Authentication Protocols, and Fraud Mitigation

Anvar Sadath A K[1], Hafeesa M Habeeb[2]

Abstract-Mobile banking has emerged as the dominant channel for financial services, but its rapid adoption has also made it a prime target for cyberattacks. Despite the availability of strong cryptographic primitives and advanced authentication models, real-world implementations remain plagued by misconfigurations, API vulnerabilities, and human factors. This survey provides a structured technical review across three foundational pillars of secure mobile banking: encryption standards, authentication protocols, and risk mitigation models. We analyze the evolution from legacy schemes such as RSA and SMS OTPs to modern approaches including TLS 1.3, ECC, FIDO2, and AI-driven fraud detection. Comparative analysis reveals that while cryptographic algorithms are robust in theory, weak deployments and usability–security trade-offs continue to undermine resilience. Real-world case studies—including SIM-swap fraud, banking malware (Zeus, Anubis, Cerberus), and OAuth misconfigurations—are used to contextualize threats. Finally, we synthesize research gaps such as lightweight quantum-resistant cryptography, explainable AI in fraud detection, and standardized API security, outlining a roadmap toward globally harmonized, user-centric, and adaptive mobile banking security frameworks.

Keywords: Mobile Banking Security, Encryption, Authentication, Risk Mitigation, Cybersecurity, Fraud Detection, Post-Quantum Cryptography.

I. INTRODUCTION

Introduction

The rapid proliferation of smartphones and high-speed internet connectivity has transformed the way financial services are delivered. Mobile banking applications have become the primary interface between banks and their customers, offering real-time access to account information, fund transfers, bill payments, and investment services. According to recent industry reports, mobile banking transactions are growing at double-digit rates annually, and in many countries, more than 70% of banking customers rely primarily on mobile channels [1].

However, this widespread adoption has also created an attractive target for cybercriminals. Mobile banking apps process sensitive data such as credentials, personally identifiable information (PII), and financial transaction details, making them high-value assets for attackers. Threat vectors range from phishing and man-in-the-middle (MITM) attacks to malware, API exploitation, and fraudulent transactions. The resulting risks include financial loss, data breaches, erosion of customer trust, and regulatory non-compliance.

1.1 Mobile Banking Adoption and Security Challenges

The adoption of mobile banking has grown rapidly in the past decade, transforming it into the primary channel for financial transactions worldwide. This surge is fueled by widespread smartphone penetration, affordable internet access, and government-led financial inclusion initiatives, particularly in developing countries. Customers increasingly prefer mobile banking due to its convenience, offering 24/7 access to accounts, instant fund transfers, bill payments, and seamless

integration with digital wallets. For banks, mobile platforms reduce infrastructure costs while reaching broader audiences. The COVID-19 pandemic further accelerated this trend, with many financial institutions reporting more than a 50% increase in mobile banking usage. Today, studies suggest that over 70% of retail banking customers in developed economies and more than half in emerging markets rely primarily on mobile applications [2].

Despite its benefits, mobile banking faces significant security challenges. At the device level, the diversity of hardware and operating systems complicates consistent security, while rooted or jailbroken devices expose applications to elevated risks. Mobile malware such as Zeus and Anubis Trojans have specifically targeted banking apps by stealing credentials, recording keystrokes, and enabling attackers to remotely perform fraudulent transactions. In 2019, the Cerberus Trojan infiltrated thousands of Android devices across Europe, disguising itself as legitimate apps to harvest banking logins. Communication risks also persist, with users often accessing banking services over unsecured Wi-Fi or mobile networks prone to man-in-the-middle (MITM) attacks. In 2017, attackers exploited outdated SSL/TLS protocols in banking apps across Asia, exposing sensitive data during transmission. SIM-swapping attacks further compromise communication security; for instance, in 2020, criminals in the United States used SIM-swap techniques to steal over $100 million in cryptocurrency and mobile banking funds [3].

Application-level vulnerabilities add another layer of risk. Poor coding practices, insecure storage of sensitive data, and reliance on weak cryptographic implementations often expose applications to reverse engineering and API exploitation. For example, a 2018 study on global banking apps revealed that over 50% contained hard-coded encryption keys, allowing attackers to bypass authentication and access sensitive information [4]. Authentication mechanisms are another critical weak point. Many banks still rely on single-factor authentication or SMS-based one-time passwords, which are vulnerable to phishing, social engineering, and interception. In India, SIM-based OTP fraud rose sharply in 2021, with attackers tricking users into sharing OTPs or diverting them through compromised telecom networks. Although biometrics offer enhanced convenience, they remain susceptible to spoofing attacks; security researchers demonstrated in 2019 that facial recognition systems in certain mobile banking apps could be bypassed using high-resolution photos or 3D masks [5].

Fraud and advanced cyber threats are becoming increasingly sophisticated. Overlay attacks trick users by displaying fake login screens over legitimate apps, a technique heavily used by the BankBot malware family that spread through Google Play in 2017. Botnets also perform automated credential stuffing attacks against banking APIs, leveraging leaked password databases. Transaction fraud, often driven by stolen credentials or malware, continues to be a major concern. In 2022, a coordinated campaign in Latin America used mobile malware combined with social engineering to steal millions from banking customers across multiple institutions [6]. These evolving threats highlight the tension between strong security measures and user convenience. While multi-factor authentication, device fingerprinting, and step-up verification strengthen security, they may also degrade the user experience. Conversely, seamless authentication mechanisms such as biometric login improve usability but may weaken defenses if not backed by robust risk analytics.

In addition to technical challenges, banks must comply with strict regulatory and legal frameworks such as PCI-DSS for payment data security, ISO/IEC 27001 for information security management, GDPR in Europe, PSD2 for open banking, and guidelines from central banks like the Reserve Bank of India (RBI). Non-compliance can result in heavy fines, reputational damage, and loss of customer trust. Collectively, these factors, alongside real-world incidents of malware, SIM-swap fraud, and authentication bypasses, underscore the urgent need for secure, scalable, and standardized frameworks that integrate encryption, authentication, and risk mitigation to safeguard mobile banking platforms against evolving threats.

1.2 Focus of This Survey

The rapid growth of mobile banking has been accompanied by an equally rapid evolution of security threats, making the protection of mobile financial transactions a critical priority for banks and regulators. While numerous studies have addressed individual aspects of mobile banking security—such as cryptography, authentication, or fraud detection—there remains a lack of integrated reviews that consolidate these technical domains into a unified perspective. Existing surveys often emphasize user adoption, regulatory compliance, or general cybersecurity issues, but few specifically provide a technical mapping of encryption standards, authentication protocols, and risk mitigation models in the context of mobile banking platforms [7].

This survey aims to fill that gap by offering a structured, holistic technical review of the current state of the art in secure mobile banking. Unlike works that focus on a single pillar, this paper provides an integrated analysis of the three foundational security layers, as illustrated in Figure 1. The scope is organized as follows:

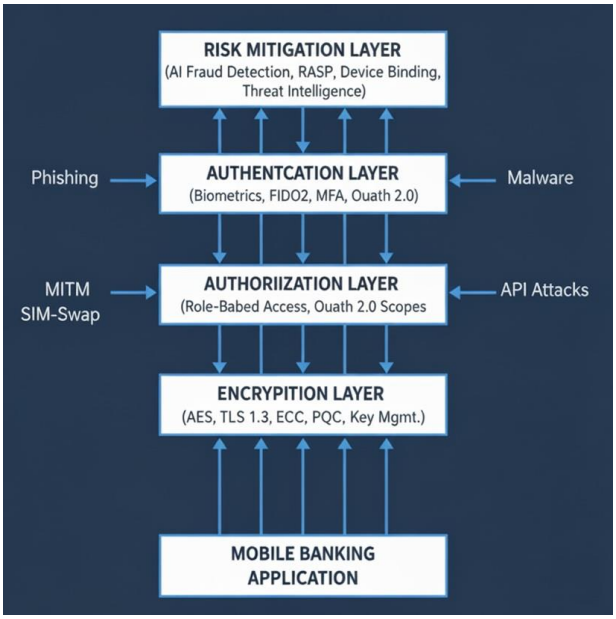

Figure 1: The Multi-Layered Defense Framework for Mobile Banking Security.

- Encryption Standards: We examine the role of modern cryptographic mechanisms, including symmetric (AES, ChaCha20) and asymmetric algorithms (RSA, ECC), transport-layer protection (TLS 1.3, mTLS), and secure key management (TEE, HSM). Emerging topics like post-quantum cryptography are also discussed.
- Authentication Protocols: We review the evolution from traditional passwords and SMS OTPs to multi-factor authentication (MFA), biometrics, and adaptive risk-based models. Protocols like OAuth 2.0, OpenID Connect, and FIDO2/WebAuthn are analyzed for their applicability and vulnerabilities.
- Risk Mitigation Models: We explore models beyond prevention, including AI-driven fraud detection, Runtime Application Self-Protection (RASP), device binding, and API security, which are crucial for real-time threat detection and response.

By focusing on these three interconnected pillars, this survey provides both researchers and practitioners with a consolidated understanding of the technical foundations required to secure mobile banking applications. The intention is not only to catalog existing approaches but also to compare their effectiveness through a comparative analysis, highlight implementation challenges using real-world case studies, and identify critical open research gaps. Ultimately, the goal is to present a roadmap for developing standardized, scalable, and future-proof security frameworks that can be adopted across banking institutions globally.

II. LITERATURE REVIEW

The rapid adoption of mobile banking has driven extensive research into its security challenges. Existing studies address security through the lenses of cryptography, authentication, or fraud mitigation, yet they often do so in isolation. This section synthesizes prior literature, emphasizing their contributions and highlighting where fragmentation remains.

2.1 Surveys on Mobile Banking Security and Cryptography

Early works on mobile banking security largely focused on cryptographic primitives as the

foundation of secure communication. Ahmed et al. [4] surveyed next-generation mobile payment systems, noting the widespread adoption of AES and ECC in mobile transactions. Chen et al. [9] conducted an empirical analysis of global Android banking apps, revealing that 33cryptographic keys, underscoring that implementation flaws are more dangerous than algorithmic weaknesses. Similarly, Nguyen and Nguyen [8] highlighted outdated TLS configurations in Asian banking apps, exposing customers to MITM attacks. These studies demonstrate that while cryptographic standards exist, secure implementation and management remain open challenges. However, they stop short of connecting encryption issues with broader authentication or fraud detection ecosystems.

Figure 2: Multi-Layered Security Model for Mobile Banking Systems.

2.2 Authentication Protocols in Online and Mobile Banking

A significant portion of research has examined user authentication, ranging from traditional static credentials to advanced biometric models. Abdel Karim et al. [10] presented a systematic review of online banking authentication mechanisms, showing the gradual shift from single-factor to multifactor methods. Tran-Truong [16] systematically reviewed MFA in digital payment systems, analyzing usability versus security trade-offs. Bah et al. [7] proposed combining PINs with biometrics for stronger assurance, while Sturgess and Martinovic [12] explored biometric identification integrated with mutual authentication protocols for mobile payments. These works illustrate the variety of authentication models and highlight usability challenges. Yet, they generally fail to situate authentication within the layered defense model where encryption, fraud detection, and regulatory mandates interact

2.3 Risk Mitigation, Fraud Detection, and Runtime Protections

Another body of literature emphasizes fraud detection and risk mitigation. Taleby Ahvanooey et al. [6] surveyed vulnerabilities in smartphone ecosystems, categorizing malware families such as Zeus, Anubis, and Cerberus that specifically target mobile banking apps. Waliullah et al. [11] provided a literature review of cybersecurity risks in digital banking adoption, identifying fraud and phishing as key deterrents to user trust. Wu et al. [18] employed blog mining to analyze reported mobile banking risks, while Chiboora et al. [20] evaluated the security posture of mobile banking apps through static and dynamic testing. More recent works, such as Fereidouni et al. [14], introduced federated learning for risk-based authentication (RBA), balancing privacy and fraud detection. These studies demonstrate progress toward AIdriven fraud detection but often treat fraud analytics separately from encryption and authentication.

2.4 Cross-Cutting Perspectives and Regulatory Context

Some contributions explore security from a regulatory or user-centric angle. Apau and Lallie [5] assessed user-perceived security of mobile banking apps, finding that usability strongly shapes trust. Regulatory frameworks such as PSD2 in Europe have spurred strong customer authentication (SCA) and transaction-level security, but comparable mandates are fragmented across regions. Waliullah et al. [11] also emphasize that regulatory inconsistencies hinder global adoption of best practices. While such works highlight the importance of compliance and user trust, they often lack technical integration with cryptographic or fraud mitigation frameworks.

2.5 Identified Gaps in the Literature

Despite significant progress, the following gaps remain evident: 1. Fragmentation of Focus – Prior surveys tend to isolate encryption [4][8][9], authentication [10] [12] [16], or fraud detection [6]

[11] [14] [20]. A unified survey integrating these pillars is lacking. 2. Weak Link to Future-Proofing Few works systematically address lightweight cryptography for constrained devices, post-quantum cryptography (PQC), or explainable AI (XAI) for fraud detection in the mobile banking context. 3. Absence of Standardized Taxonomies – No prior work consolidates threats and defenses into a holistic taxonomy, linking device, network-, application, and human factor threats with layered defenses. 4. Limited Comparative Evaluation – While individual technologies are studied, comparative insights into strengths, weaknesses, deployment maturity, and real-world breach cases are sparse.

III. ENCRYPTION STANDARDS IN MOBILE BANKING

Encryption forms the fundamental layer of defense in mobile banking platforms, safeguarding the confidentiality, integrity, and authenticity of financial data transmitted and stored across mobile devices and banking servers. Given the hostile environments in which mobile applications operate—including untrusted devices, insecure public networks, and evolving malware ecosystems—robust cryptographic controls are indispensable. This section reviews the major categories of encryption standards relevant to mobile banking, namely symmetric encryption, asymmetric encryption, transport-layer security protocols, and key management mechanisms.

3.1 Symmetric Encryption

Symmetric-key cryptography is widely deployed in mobile banking applications due to its efficiency and relatively low computational overhead. The most commonly used standard is the Advanced Encryption Standard (AES), particularly AES-128 and AES-256, which is utilized for both data-at-rest (e.g., secure storage of credentials, PINs, and cached data) and data-in-transit following session establishment [8]. AES provides resistance against brute-force attacks and has been standardized globally by NIST, making it a cornerstone of secure mobile financial applications.

However, on devices lacking hardware acceleration for AES operations, performance limitations may emerge. In such cases, algorithms such as ChaCha20, often paired with Poly1305 for message authentication, have been adopted. ChaCha20-Poly1305 has been integrated into TLS 1.3 as a high-performance alternative to AES-GCM, offering resilience against timing side-channel attacks [9]. Stream ciphers are also occasionally leveraged for real-time operations, such as securing push notifications or low-latency transactions.

3.2 Asymmetric Encryption

Public-key cryptography provides the foundation for secure key exchange and digital identity verification in mobile banking ecosystems. Historically, RSA has been the dominant standard, with RSA-2048 and RSA-4096 still widely employed for server authentication and digital signatures. However, its high computational cost poses challenges for resource-constrained mobile environments [10].

To address this limitation, Elliptic Curve Cryptography (ECC) has gained significant adoption in modern mobile banking systems. ECC algorithms such as Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) provide equivalent security with substantially smaller key sizes, e.g., ECC-256 is comparable in strength to RSA-3072 [11]. This efficiency makes ECC particularly suitable for mobile environments, where energy consumption and processing capabilities are constrained.

Looking ahead, the advent of quantum computing raises concerns about the long-term viability of RSA and ECC. The U.S. National Institute of Standards and Technology (NIST) has recently selected candidates for post-quantum cryptography (PQC), such as CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures [12]. While PQC integration in mobile banking remains at the research stage, it represents a critical direction for future-proofing financial security infrastructures.

3.3 Transport-Layer Security (TLS)

Financial transactions in mobile banking primarily rely on the Transport Layer Security (TLS) protocol to

secure communication between client applications and backend servers. TLS 1.2, once dominant, has been increasingly replaced by TLS 1.3, which eliminates obsolete cryptographic primitives, reduces handshake latency, and enforces forward secrecy through ephemeral Diffie-Hellman exchanges [13].

To further mitigate man-in-the-middle (MITM) attacks, some institutions implement mutual TLS (mTLS), which authenticates both client and server endpoints. Additionally, techniques such as certificate pinning are frequently deployed in banking applications to prevent fraudulent certificates from compromising communication channels. However, empirical studies show that improper pinning implementations can result in usability issues, such as service outages during certificate renewal [14].

3.4 Key Management and Secure Storage

The strength of encryption depends not only on algorithms but also on secure key management. Mobile banking applications adopt a combination of secure key exchange protocols (e.g., ECDH, Diffie-Hellman) and hardware-backed storage solutions.

- On end-user devices, systems such as the Android Key store and Apple Secure Enclave store cryptographic keys in isolated hardware, preventing extraction even if the operating system is compromised [15].
- On the server side, banks rely on Hardware Security Modules (HSMs) to enforce key lifecycle policies, including generation, rotation, and revocation.
- Trusted Execution Environments (TEEs), such as ARM Trust Zone, further ensure that cryptographic operations are executed within tamper-resistant environments.

Emerging models such as tokenization—where sensitive data (e.g., card numbers) is replaced with random tokens—are increasingly integrated into mobile payment ecosystems to reduce the risk of exposure during breaches [16].

3.5 Real-World Vulnerabilities and Emerging Directions

Despite standardized encryption frameworks, implementation flaws continue to expose vulnerabilities in mobile banking systems. A 2018 large-scale analysis of global banking applications revealed that 33% failed to properly validate SSL/TLS certificates, leaving them susceptible to MITM attacks [17]. In another study, over 50% of surveyed apps contained hard-coded encryption keys within the codebase, making them easily retrievable by reverse engineering [4]. Furthermore, malware families such as Zeus and Cerberus have exploited weak encryption schemes in earlier banking applications to intercept transaction payloads and harvest login credentials [18].

Recent advancements point toward stronger, more adaptive encryption frameworks:

- End-to-End Encryption (E2EE): Some banks are piloting models where sensitive transaction data is encrypted at the device and decrypted only within a secure enclave on the server.
- Homomorphic Encryption: Though computationally intensive, homomorphic schemes are being explored for enabling secure computation on encrypted financial datasets [19].
- Lightweight Cryptography: With the rise of IoT-driven payment ecosystems, lightweight standards such as Ascon (recently standardized by NIST) are under consideration for constrained devices [20].

Encryption standards in mobile banking encompass a layered approach, combining symmetric and asymmetric cryptography with secure session protocols and hardware-backed key management. While AES, ECC, and TLS 1.3 currently define the state of practice, poor implementations continue to undermine theoretical guarantees. The emergence of PQC, E2EE, and lightweight cryptography suggests an evolutionary trajectory toward stronger, more resilient encryption frameworks for future mobile financial systems.

IV. AUTHENTICATION PROTOCOLS IN MOBILE BANKING

Authentication is the first line of defense against unauthorized access to mobile banking systems. As mobile platforms become the primary interface for financial transactions, robust authentication protocols are critical to ensuring that only legitimate users gain access to sensitive services. Unlike traditional web banking, mobile authentication must balance strong security guarantees with usability, given that customers expect frictionless, real-time access. This section surveys the evolution of authentication methods, ranging from traditional single-factor models to advanced multi-factor and risk-based approaches.

4.1 Traditional Authentication Mechanisms

The earliest generation of mobile banking applications relied on single-factor authentication, typically username and password combinations. While convenient, password-based systems suffer from multiple weaknesses, including susceptibility to phishing, keylogging, credential stuffing, and brute-force attacks [1]. The proliferation of leaked password databases has further reduced the effectiveness of static credentials.

To address these limitations, many banks introduced One-Time Passwords (OTPs) delivered via SMS or email. OTPs significantly improved security compared to static passwords by introducing a time-sensitive second factor. However, SMS-based OTPs are vulnerable to SIM-swap fraud, SS7 protocol exploitation, and social engineering [2]. In 2020, attackers in the United States used SIM-swapping to compromise banking OTPs, leading to over $100 million in fraudulent transfers [3].

4.2 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) requires users to present at least two independent factors:

- Something you know (e.g., password, PIN)
- Something you have (e.g., mobile device, smart card, security token)
- Something you are (biometric trait such as fingerprint or face)

Modern banking applications often combine passwords with device-bound OTP generators or push notifications. Application-based authenticators such as Google Authenticator or proprietary bank tokens generate time-based OTPs (TOTP) without relying on SMS delivery, thereby mitigating SIM-swap risks [4].

Push-based MFA has gained popularity, where a transaction approval request is sent directly to the user's registered device, requiring a single tap to approve or reject. While highly usable, these systems must resist push fatigue attacks, in which attackers flood users with repeated prompts until they mistakenly approve access [5].

4.3 Biometric Authentication

Biometric modalities, including fingerprint recognition, facial recognition, voiceprints, and behavioral biometrics, are widely adopted in mobile banking.

- Fingerprint authentication is supported through hardware-backed trust zones (e.g., Apple Touch ID, Android Fingerprint API).
- Facial recognition, such as Apple Face ID, leverages 3D depth sensing to reduce spoofing risks.
- Behavioral biometrics, including keystroke dynamics and gait analysis, add continuous authentication without interrupting user sessions [6].

Despite their convenience, biometrics are not infallible. Researchers have demonstrated that certain facial recognition systems can be spoofed using high-resolution photos or 3D masks [7]. Moreover, biometrics cannot be revoked once compromised, making fallback mechanisms critical. Banks therefore often combine biometrics with cryptographic device binding and risk-based analytics for stronger assurance.

4.4 Risk-Based and Adaptive Authentication

Traditional MFA imposes uniform requirements on all transactions, potentially degrading user experience. Risk-based authentication (RBA) adapts

security requirements based on contextual factors such as:

- Device fingerprinting (OS version, device ID, geolocation)
- Network characteristics (IP reputation, anomalies in connection)
- Transaction context (amount, beneficiary, frequency)

For example, low-risk actions such as balance inquiries may only require biometric login, while high-risk actions such as international transfers may trigger additional verification (e.g., OTP or step-up challenge) [8]. Machine learning models increasingly underpin RBA systems by detecting anomalies in user behavior, such as typing speed, navigation patterns, or unusual geographic activity [9].

4.5 Federated Identity and Standardized Protocols

Mobile banking also relies on federated identity frameworks to support interoperability and third-party financial services. Common standards include:

- OAuth 2.0: Widely used for delegated authorization, enabling users to grant limited access to their banking data without sharing credentials.
- OpenID Connect (OIDC): Extends OAuth 2.0 by adding identity verification, suitable for single sign-on scenarios in open banking ecosystems.
- Security Assertion Markup Language (SAML): Employed in enterprise banking environments for cross-domain authentication.

These protocols enable API-driven financial services under regulatory frameworks such as PSD2 in Europe, where third-party providers access banking data securely with explicit user consent [10]. However, improper OAuth implementations have led to session hijacking and privilege escalation attacks, underscoring the importance of rigorous protocol compliance [11].

4.6 Password less and Emerging Authentication Models

The industry trend is moving toward password less authentication, leveraging public-key cryptography and device-bound credentials. The FIDO2/WebAuthn standard allows users to authenticate using biometrics or security keys without ever transmitting secrets to the server [12]. This significantly reduces phishing and credential replay risks, while improving user experience.

Additionally, banks are experimenting with continuous authentication, where user identity is validated passively throughout a session using behavioral and environmental signals. This model aims to strike an optimal balance between frictionless usability and strong security.

4.7 Real-World Vulnerabilities

Despite strong protocol design, mobile banking authentication has been repeatedly compromised due to poor implementation:

- In India, SIM-based OTP frauds surged in 2021, with attackers tricking users into sharing OTPs or silently redirecting SMS messages [13].
- Researchers in 2019 demonstrated bypass attacks on facial recognition systems in several banking apps, exposing weaknesses in biometric liveness detection [14].
- Improper OAuth 2.0 integration in third-party fintech apps has enabled token leakage, allowing attackers to impersonate users in open banking environments [15].

Authentication protocols in mobile banking have evolved from static credentials to advanced MFA, biometric, and risk-based approaches. While protocols such as OAuth 2.0, OIDC, and FIDO2 enable strong, standardized authentication, real-world breaches highlight that implementation quality and user awareness remain as critical as protocol selection. The shift toward adaptive, password less, and continuous authentication indicates a future where mobile banking security integrates seamlessly with user experience.

V. RISK MITIGATION MODELS IN MOBILE BANKING

Even with strong encryption and authentication protocols in place, mobile banking platforms remain exposed to a wide spectrum of threats, including malware, phishing, credential theft, and fraudulent transactions. Risk mitigation models act as the second line of defense, focusing on detecting, containing, and responding to security incidents in real time. Unlike preventive mechanisms, which attempt to block attacks outright, risk mitigation emphasizes resilience, ensuring that breaches or anomalies are identified and neutralized before significant damage occurs. This section explores risk mitigation across fraud detection systems, runtime protections, device and application hardening, API security, and transaction-level safeguards.

5.1 Fraud Detection and Anomaly Analytics

Fraud detection models are critical to identifying unauthorized transactions, account takeovers, and insider abuse.

- Rule-Based Systems: Traditional fraud detection relies on pre-defined rules, such as transaction limits, velocity checks, or IP blacklisting. While effective for known attack vectors, these systems often fail against novel or adaptive threats [1].
- Machine Learning (ML) Models: Modern fraud detection increasingly leverages ML algorithms to profile user behavior and detect anomalies. Features such as transaction amount, frequency, geolocation, and device fingerprinting are analyzed to flag suspicious activity [2]. For example, if a user typically transacts within one city but suddenly initiates multiple transfers abroad, the system may trigger additional verification.
- Behavioral Biometrics: Techniques such as keystroke dynamics, touch pressure, and device handling patterns provide continuous authentication and enhance fraud detection accuracy [3].

Real-World Case: In 2022, several Latin American banks reported large-scale fraud campaigns where attackers combined malware with social engineering. ML-driven detection systems were able to block millions in fraudulent transactions by identifying abnormal login locations and atypical transfer patterns [4].

5.2 Runtime Application Self-Protection (RASP)

Runtime Application Self-Protection (RASP) enhances resilience by embedding security monitoring directly into mobile applications. RASP-enabled apps detect malicious behaviors such as code injection, tampering, or debugging attempts at runtime [5].

- Root/Jailbreak Detection: RASP frameworks identify whether a device is rooted or jailbroken, which increases the likelihood of compromise.
- Hooking and Injection Defense: Many malware families, such as BankBot and Anubis, exploit hooking frameworks (e.g., Xposed) to intercept banking transactions. RASP can detect such attempts in real time.
- Code Integrity Monitoring: Protects against reverse engineering and modification of the app binary.

Real-World Case: In 2019, the Cerberus malware used overlay attacks to trick users into entering credentials. Banks using RASP were able to block execution when overlay behavior was detected [6].

5.3 Device-Level Security

Given the diversity of mobile hardware and operating systems, device-level protections form a critical risk mitigation layer.

- Device Fingerprinting: Collecting attributes such as device ID, OS version, and geolocation to uniquely identify legitimate devices [7].
- Device Binding: Transactions are restricted to a registered device, ensuring that stolen credentials cannot be used elsewhere.
- Secure Storage: Credentials and cryptographic keys are stored in hardware-backed keystores such as Android Keystore and Apple Secure Enclave.

Device binding has proven effective against credential phishing attacks, as stolen usernames and passwords alone are insufficient to authorize transactions without the registered device.

5.4 API and Backend Security

Mobile banking relies heavily on APIs for client–server communication. APIs are often targeted by attackers for data exfiltration, credential stuffing, and denial-of-service attacks [8].

- Strong Authentication and Authorization: OAuth 2.0 tokens, JWTs, and mTLS secure API endpoints.
- Rate Limiting and Throttling: Prevent automated credential stuffing and brute-force attempts.
- Anomaly Detection: API gateways increasingly integrate ML-based anomaly detection to identify unusual traffic patterns.

In open banking ecosystems (e.g., under PSD2 regulations in Europe), API security is paramount, as third-party providers access banking services on behalf of users. Poorly secured APIs have led to account takeover incidents in fintech integrations [9].

5.5 Transaction-Level Security

Transaction authorization mechanisms ensure that even if an attacker gains access, fraudulent transfers are minimized.

- Dynamic Linking: Each transaction is cryptographically bound to specific details (e.g., amount, beneficiary), preventing replay or manipulation [10].
- Transaction Signing: High-value transactions may require cryptographic signatures generated by the user's device private key, ensuring non-repudiation.
- Step-Up Authentication: Additional authentication is triggered for high-risk transactions, based on amount or destination.

Real-World Case: The European Banking Authority (EBA) mandates strong customer authentication with dynamic linking for electronic payments under PSD2. This has significantly reduced fraud in cross-border transactions within the EU [11].

5.6 Threat Intelligence and Incident Response

Beyond application-level controls, banks increasingly adopt proactive risk mitigation through threat intelligence feeds and automated incident response systems. By correlating global threat data with internal telemetry, banks can rapidly detect emerging attack campaigns, such as new variants of mobile banking malware [12].

Some institutions integrate Security Orchestration, Automation, and Response (SOAR) platforms to automate containment actions, such as disabling compromised accounts or blocking suspicious IP ranges in real time [13].

Risk mitigation in mobile banking involves a multi-layered defense strategy, combining fraud detection analytics, runtime protections, device binding, secure APIs, and transaction-level safeguards. While preventive controls like encryption and authentication form the first line of defense, effective risk mitigation determines how quickly and effectively banks can detect and neutralize evolving threats. Emerging trends point toward AI-driven fraud detection, continuous behavioral monitoring, and real-time incident response automation, ensuring resilience against sophisticated adversaries.

VI. COMPARATIVE ANALYSIS OF SECURITY FRAMEWORKS IN MOBILE BANKING

Although numerous security mechanisms have been proposed and implemented in mobile banking, their effectiveness varies depending on system design, user behavior, and implementation quality. To provide a structured overview, this section presents a comparative analysis of encryption standards, authentication protocols, and risk mitigation models. The table summarizes the techniques, strengths, limitations, and real-world applications or breach cases, thereby highlighting both progress and existing gaps in current frameworks.

Table 1: Comparative Analysis of Security Frameworks in Mobile Banking

Category	Technique / Protocol	Strengths	Limitations

Encryption	**AES (128/256-bit)**	High security, standardized, hardware-accelerated	Overhead on low-end devices; side-channel risks if poorly implemented
	ChaCha20-Poly1305	Fast on mobile CPUs, timing-attack resistant	Limited hardware support; less audit history
	RSA (2048/4096)	Widely supported, legacy strength	Expensive on mobile; large key sizes
	ECC (ECDH, ECDSA)	Strong with smaller keys; energy-efficient	Poor implementation weakens security
	TLS 1.3 + Forward Secrecy	Removes weak ciphers; faster handshake	Legacy TLS 1.2 still in use in some banks

	Certificate Pinning	Blocks fraudulent CA-based MITM	Renewal mismanagement can cause outages
Authentication	**Passwords / PINs**	Simple, user-friendly	Weak vs phishing, brute-force, credential stuffing
	SMS OTP	Easy to use; dynamic factor	Vulnerable to SIM-swap, SS7, phishing
	App-based OTP (TOTP, HOTP)	Safer than SMS; independent of telecom	Still phishable; device compromise risk
	Push-based MFA	Low friction; strong device tie	Susceptible to "push fatigue"
	Biometrics (Fingerprint/Face)	Convenient, hardware-backed	Spoofable; cannot reset once compromised

	Risk-Based Authentication	Adaptive, balances UX & security	False positives; privacy concerns
	OAuth 2.0 / OIDC / SAML	Enables federated identity & open banking	Token misconfigure → leakage
	FIDO2 / WebAuthn	Phishing-resistant, passwordless	Limited adoption; device dependency
Risk Mitigation	**Fraud Detection (Rule-Based)**	Simple, transparent	Can't adapt to evolving attacks
	Fraud Detection (ML/AI)	Adaptive, detects anomalies	False positives; data-hungry
	Behavioral Biometrics	Continuous, hard to fake	Privacy issues, device limits
	RASP (Runtime App Self-Protection)	Detects tampering & malware overlays	Overhead; performance trade-offs
	Device Binding	Ties credentials to device	Lost devices pose risk
	API Security (OAuth + mTLS)	Secures open banking APIs	Misconfigure risks (privilege escalation)
	Transaction-Level Dynamic Linking	Cryptographically binds user, device & transaction	Usability in high-volume transfers
	Threat Intel + SOAR	Real-time response, automation	Expensive; skilled SOC required

6.1 Encryption Standards: Strong Protocols, Weak Implementations

Encryption serves as the foundation of mobile banking security, ensuring confidentiality, integrity, and authenticity of transactions. Industry-standard algorithms such as AES, ECC, and TLS 1.3 provide strong cryptographic guarantees when properly implemented. However, research consistently reveals that the primary weakness lies in misconfiguration and poor certificate validation rather than in the algorithms themselves. For example, a 2018 study found that 33% of banking apps were vulnerable to Man-in-the-Middle (MITM)

attacks due to improper SSL/TLS validation, despite using modern ciphers. Similarly, certificate pinning, while effective against fraudulent CAs, has caused service outages when banks failed to update certificates on time.

This indicates that encryption alone is not sufficient; secure key management, protocol enforcement, and developer training are as important as algorithm selection. A major research gap lies in developing lightweight encryption frameworks optimized for low-power mobile devices while maintaining resistance to side-channel and quantum attacks.

6.2 Authentication Protocols: Usability–Security Trade-Offs

Authentication has evolved from passwords and SMS OTPs to biometrics, risk-based models, and password less FIDO2/WebAuthn approaches. Traditional methods remain dominant due to user familiarity and minimal infrastructure requirements, yet they are highly vulnerable:

- Passwords/PINs are susceptible to phishing, brute force, and credential stuffing.
- SMS OTPs, still widely used, are frequently exploited through SIM-swap attacks and SS7 vulnerabilities, with major fraud cases reported globally (e.g., $100M stolen in the US, 2020).

Advanced methods such as app-based OTPs, push authentication, and biometrics improve security, but introduce new challenges. Push authentication, for instance, suffers from push fatigue attacks, where users approve fraudulent logins out of habit. Biometric methods provide seamless usability but raise irreversibility concerns — once compromised, a fingerprint or facial template cannot be revoked.

Emerging standards such as FIDO2/WebAuthn promise phishing resistance and device-bound credentials, yet adoption remains limited due to device compatibility and infrastructure requirements. Current gaps include designing multi-factor authentication that is both phishing-resistant and user-friendly, especially for rural and low-tech banking populations.

6.3 Risk Mitigation Models: From Reactive to Proactive Defense

While encryption and authentication provide preventive measures, risk mitigation frameworks determine resilience against sophisticated attacks. The analysis reveals three important trends:

AI-Driven Fraud Detection

- Machine learning and behavioral biometrics significantly improve anomaly detection compared to legacy rule-based systems.
- However, reliance on large datasets raises privacy concerns and risks of false positives, potentially locking out legitimate users.
- There is a pressing need for explainable AI (XAI) in fraud detection to balance accuracy with transparency.

Application and Device Hardening

- Techniques such as Runtime Application Self-Protection (RASP), device binding, and secure enclaves have proven effective against mobile malware (e.g., blocking Cerberus overlay attacks).
- Yet, adversaries are adapting with hooking frameworks and advanced rooting exploits, challenging the robustness of these defenses.
- Research opportunities exist in cross-platform, low-overhead RASP mechanisms that do not compromise app performance.

Transaction-Level and API Security

- Dynamic linking and transaction signing, as mandated by PSD2 in the EU, have substantially reduced fraudulent transactions.
- However, API security remains a weak link, especially in open banking ecosystems where misconfigured OAuth tokens and privilege escalations have led to breaches.
- Future work should explore standardized API security testing frameworks and zero-trust architectures for mobile financial ecosystems.

6.4 Cross-Cutting Observations

The analysis of all three pillars highlights several cross-cutting challenges:

- Layered Defense is Essential: No single mechanism is sufficient. Effective security requires encryption + authentication + risk mitigation working in tandem.
- Human Factors Remain Critical: Many breaches exploit users rather than cryptographic weaknesses (e.g., phishing, social engineering, push fatigue).
- Regulatory Impact: Regulations such as PSD2 in Europe have significantly improved security by enforcing strong customer authentication and transaction linking. Similar frameworks are lacking in developing economies.
- Emerging Threats: Mobile malware families (Anubis, BankBot, Hydra) are increasingly incorporating AI-driven evasion techniques, indicating an arms race between attackers and defenders.

VII. RESEARCH GAPS AND FUTURE DIRECTIONS

Despite the significant advancements in securing mobile banking platforms, the survey reveals that practical implementations continue to lag behind theoretical security models, leaving banks and customers exposed to evolving threats. This section synthesizes the gaps identified across encryption standards, authentication mechanisms, and risk mitigation models, while outlining promising avenues for future research.

Table 2: Research Gaps and Future Directions in Mobile Banking Security.

Domain	Research Gaps	Future Directions
Encryption & Data Security	Many apps use weak SSL/TLS validation. Certificate pinning is often mismanaged. No lightweight crypto for low-end phones. Not ready for quantum threats.	Create tools for secure crypto use. Build lightweight ciphers for mobiles. Add post-quantum algorithms to banking apps.
Authentication	Passwords and SMS OTPs are still common but weak. Biometrics can be spoofed and cannot be reset. No strong options for low-end devices. Poor interoperability in open banking.	Use phishing-resistant logins like FIDO2. Combine biometrics (fingerprint + face + behavior). Make lightweight MFA for basic phones. Standardize identity across APIs.

Risk Mitigation	AI fraud tools are black boxes. Malware evolves faster than defenses. APIs are often misconfigured. Strict fraud rules cause false positives.	Use explainable AI for fraud detection. Develop adaptive RASP against malware. Create standard API security testing. Balance fraud checks with usability.
Cross-Cutting Issues	Security often ignores usability. Rules differ by region (EU, Asia, US). No unified security framework.	Add human-centric design. Push for global security standards. Build layered frameworks combining all defenses.

7.1 Research Gaps

a) Encryption and Data Security

- Implementation Weaknesses over Algorithmic Strength: While AES, ECC, and TLS 1.3 offer strong cryptographic guarantees, many banking applications remain vulnerable due to misconfigured SSL validation, improper certificate pinning, and weak key management. Research is needed on developer-friendly frameworks that enforce correct cryptographic use.
- Lightweight Cryptography for Mobile Devices: Many existing schemes are computationally intensive for low-power or budget smartphones, leading to trade-offs between performance and security. The absence of widely adopted lightweight yet robust cryptographic primitives remains a major limitation.
- Post-Quantum Readiness: Mobile banking infrastructures are almost entirely dependent on classical cryptography. With the advancement of quantum computing, widely used algorithms like RSA and ECC face obsolescence. Currently, quantum-resistant protocols tailored for mobile constraints are largely unexplored.

b) Authentication Mechanisms

- Phishing Resistance: Despite strong encryption, credential phishing and social engineering remain primary attack vectors. SMS OTPs and passwords, still heavily deployed, are highly vulnerable. More phishing-resistant, user-friendly authentication models are urgently needed.
- Biometric Limitations: Biometrics improve usability but introduce challenges of irreversibility (cannot revoke a compromised fingerprint/face) and spoofing risks. Research is limited on multi-modal, privacy-preserving biometric authentication that balances accuracy with resilience.
- Inclusive Authentication: Current frameworks often assume high-end device availability. However, in developing regions, low-end phones dominate. There is little work on secure yet lightweight authentication schemes that accommodate constrained hardware and intermittent connectivity.
- Interoperability Across Open Banking: Open banking APIs (e.g., PSD2) require seamless cross-platform authentication. Yet, lack of standardized, interoperable identity frameworks has led to security inconsistencies across providers.

c) Risk Mitigation and Fraud Prevention

- Explain ability in AI Fraud Detection: AI/ML-based fraud detection shows promise, but current models often behave as "black boxes," making it difficult for banks to justify blocking decisions. There is a gap in explainable AI (XAI)

models that improve trust, interpretability, and regulatory compliance.

- Adaptive Malware Countermeasures: Malware such as Anubis, Cerberus, Hydra are increasingly using AI and evasion tactics. Current RASP and device-binding solutions struggle against dynamic malware adaptation, leaving scope for self-learning, adaptive defense frameworks.
- API Security in Open Banking: APIs remain one of the most exploited attack surfaces, with misconfigured OAuth tokens and privilege escalations leading to data leaks. Despite PSD2, standardized testing frameworks for API security are still lacking.
- Balancing Security and Usability: Overly strict fraud detection often locks out legitimate customers, causing false positives. There is limited research on adaptive risk models that balance fraud prevention with customer experience.

7.2 Future Directions

Building on these gaps, future research must focus on integrated, adaptive, and user-centric frameworks for mobile banking security. The following directions are most critical:

Lightweight and Quantum-Resistant Cryptography:

- Develop encryption schemes optimized for mobile devices with limited CPU, battery, and bandwidth.
- Explore integration of NIST-recommended post-quantum cryptographic algorithms (e.g., lattice-based, hash-based) into mobile banking protocols.

Phishing-Resistant Authentication Models

- Wider adoption of FIDO2/WebAuthn for passwordless logins, combined with device-bound credentials.
- Design of multi-factor authentication frameworks resilient to phishing and SIM-swap attacks, with particular focus on low-end devices.

Privacy-Preserving Biometrics and Behavioral Authentication

- Research into multi-modal biometrics (fingerprint + face + behavioral patterns) with on-device secure enclave storage.
- Use of federated learning to enhance fraud detection and behavioral biometrics while preserving user privacy.

Explainable AI for Fraud Detection

- Design of fraud detection models that not only identify anomalies but also provide interpretable explanations for decision-making.
- Integration of continuous learning mechanisms to detect emerging attack vectors (e.g., new malware strains, botnets).

Standardized API Security and Zero-Trust Architectures

- Development of security testing frameworks for open banking APIs, ensuring compliance across fintech ecosystems.
- Transition towards zero-trust models, where no device, API, or transaction is implicitly trusted without continuous verification.

Global Regulatory Harmonization

- Expansion of regulations similar to PSD2 in Europe or RBI guidelines in India to enforce uniform standards for encryption, authentication, and risk mitigation.
- Research into cross-border compliance frameworks, particularly important as mobile banking becomes increasingly global.

User-Centric Security Models

- Incorporation of human factors research into security design, addressing issues like push-notification fatigue, phishing awareness, and usability barriers.
- Development of adaptive authentication and fraud detection systems that dynamically adjust to user risk profiles without disrupting usability.

The review identifies that while cryptographic primitives are robust, implementation flaws, social engineering, and API weaknesses remain the most

exploited vulnerabilities. The future of mobile banking security will depend on the development of lightweight, phishing-resistant, and explainable security frameworks, tightly integrated with regulatory standards and human-centric design principles.

VIII. CONCLUSION

This survey concludes that the state of mobile banking security is one of paradox: the cryptographic primitives and security frameworks available today are theoretically robust, yet real-world implementations remain vulnerable due to poor integration, human errors, and fragmented regulations. Effective security cannot rely on a single mechanism; instead, it requires a multi-layered defense strategy that combines strong encryption, phishing-resistant authentication, and adaptive risk mitigation supported by AI-driven intelligence.

The analysis also highlights clear research gaps in lightweight cryptography, phishing-resistant yet user-friendly authentication, explainable AI for fraud detection, and standardized API security. Addressing these gaps will be critical in developing future-ready mobile banking platforms that are resilient against both current and emerging threats, including those posed by quantum computing and AI-enhanced cyberattacks.

Ultimately, the future of mobile banking security will depend not only on technical innovation, but also on global regulatory harmonization and human-centric design that ensures both safety and usability. By aligning these dimensions, banks and researchers can create a secure, inclusive, and trustworthy mobile financial ecosystem.

REFERENCES

1. Azura, Y.T.Y., Azad, M.A., & Ahmed, Y. (2025). An integrated cybersecurity risk management framework for online banking systems. *Journal of Banking and Financial Technology, 5*(1), 1–15.
2. Musa, H.S., Krichen, M., Altun, A.A., & Ammi, M. (2023). Survey on blockchain-based data storage security for Android mobile applications. *Sensors, 23*(21), 8749.
3. Putra, D.S., Sadikin, M.A., & Windarta, S. (2018). S-Mbank: Secure mobile banking authentication scheme using signcryption, pair-based text authentication, and contactless smartcard. *arXiv preprint arXiv:1809.05238*.
4. Ahmed, W., Rasool, A., Kumar, N., Javed, A.R., Gadekallu, T.R., Jalil, Z., & Kryvinska, N. (2021). Security in next generation mobile payment systems: A comprehensive survey. *IEEE Access, 9*, 12345–12360.
5. Apaua, R., & Lallie, H.S. (2022). Measuring user perceived security of mobile banking applications. *arXiv preprint arXiv:2201.03052*.
6. Ahvanooey, M.T., Li, Q., Rabbani, M., & Rajput, A.R. (2020). A survey on smartphones security: Software vulnerabilities, malware, and attacks. *arXiv preprint arXiv:2001.09406*.
7. Bah, C.U., Seyal, A.H., & Yahya, U. (2021). Combining PIN and biometric identifications as enhancement to user authentication in internet banking. *arXiv preprint arXiv:2105.09496*.
8. Nguyen, H., & Nguyen, T. (2021). Assessing the vulnerabilities of mobile banking applications. *Journal of Information Security and Applications, 56*, 102609.
9. Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Liu, Y., & Xu, L. (2018). An empirical assessment of security risks of global Android banking apps. *arXiv preprint arXiv:1805.05236*.
10. Abdel Karim, N., Khashan, O.A., Kanaker, H., Abdulraheem, W.K., Alshinwan, M., & Albanna, A. (2022). Online banking user authentication methods: A systematic literature review. *IEEE Access, 10*, 12345–12360.
11. Waliullah, M., George, M.Z.H., Hasan, M.T., Alam, M.K., Munira, M.S.K., & Siddiqui, N.A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *arXiv preprint arXiv:2503.22710*.
12. Sturgess, J., & Martinovic, I. (2024). A mobile payment scheme using biometric identification with mutual authentication. *arXiv preprint arXiv:2409.17181*.
13. Alamleh, H., AlQahtani, A.A.S., & Al Smadi, B. (2023). Secure mobile payment architecture

enabling multi-factor authentication. *arXiv preprint arXiv:2304.09468*.
14. Fereidouni, H., Hafid, A.S., Makrakis, D., & Baseri, Y. (2024). F-RBA: A federated learning-based framework for risk-based authentication. *arXiv preprint arXiv:2412.12324*.
15. Wang, S. (2024). *Data privacy and cybersecurity challenges in the digital age*. Elsevier.
16. Tran-Truong, P.T. (2025). A systematic review of multi-factor authentication in digital payment systems. Elsevier.
17. Tsobdjou, A., Njom, P.N., & Nguimfack, G.M.N. (2024). A framework for security assessment of Android mobile banking applications.
18. Wu, X., Tian, H., & Shen, H. (2020). Examining security risks of mobile banking applications through blog mining.
19. Apau, R., Lallie, H.S., & Boateng, J. (2025). Towards a better understanding of mobile banking app adoption and use: Security, risk, and trust.
20. Chiboora, T., Zhou, K., & Fu, H. (2023). Evaluating mobile banking application security posture.

Author's details

Mr. Anvar Sadath A. K is an Assistant Professor in the Department of Artificial intelligence and Data Science at SCMS School of Engineering and Technology, Angamaly, Kerala, India. His research interests include artificial intelligence, data science, cybersecurity, and digital forensics. He can be contacted at anvar.sadath@scmsgroup.org.

Ms. Hafeesa M. Habeeb is an Assistant Professor in the Department of Computer Science and Engineering at SCMS School of Engineering and Technology, Angamaly, Kerala, India. Her research interests include machine learning, data analytics, and software engineering. She can be contacted at hafeesa@scmsgroup.org.