ISSN: 2182-2069 / E-ISSN: 2182-2077

# Secure Wireless Connectivity Frameworks for Financial Internet Services

Dr.K. Vinutha[1*], Sivaprasad Lebaka[2], Mani Rajakumar[3], Zaid Ajzan Alsalami[4], Siroj Zarina Rustambekovna[5], and D. Dhanasekaran[6]

[1*]Assistant Professor, Department of ISE, BMS Institute of Technology and Management, Bengaluru, India. vinutha.k90@gmail.com, https://orcid.org/0000-0002-2165-4738

[2]Assistant Professor, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India. sivaprasadlebaka@gmail.com, https://orcid.org/0000-0002-0526-9995

[3]Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India. manirajakumar@amet-ist.in, https://orcid.org/0009-0000-3971-8456

[4]Department of Computers Techniques Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, The Islamic University of Al Diwaniyah, Al Diwaniyah, Iraq. eng.iu.zaidsalami12@gmail.com, https://orcid.org/0009-0001-8761-2565

[5]Department of Banking and Finance, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. zarina36.84@gmail.com, https://orcid.org/0009-0007-7266-3515

[6]Assistant Professor, Department of Electronics and Communication Engineering, K.S. Rangasamy College of Technology, Tiruchengode, India. dhanasekarand@ksrct.ac.in, https://orcid.org/0009-0003-2135-2451

Received: May 02, 2025; Revised: June 17, 2025; Accepted: July 30, 2025; Published: August 30, 2025

## Abstract

The emergence of wireless networks has promoted the ease, immediacy and efficiency of access and transacting financial internet services. Nonetheless, such developments offer chances of severe criminal activities, including information violations, identity theft, and data leakage. The paper reviews protective structures of financial internet services, emphasizing secure wireless convenience and connection. It evaluates the vulnerabilities of Wi-Fi, LTE, and emerging 5G wireless communication technologies concerning confidentiality, integrity, and availability of sensitive financial information. A layered security approach towards wireless transactions is proposed and it includes end-to-end encryption, multifactor authentication, VPNs and advanced intrusion detection systems (IDS). Moreover, blockchain is regarded with zero-trust frameworks to enhance trust and transparency in the financial systems. Cases of cyberattack on financial infrastructures have revealed flaws in the current systems, demonstrating vulnerabilities in current wireless security frameworks. It is based on these trends of flexibility to develop this model to articulate the policies of the electronic security in wireless networks without infringing on the standards of PCI-DSS and GDPR. The hyper-connected world enables service providers to manage risk more effectively and deliver services safely to users by introducing risk-enhancing

*Journal of Internet Services and Information Security (JISIS)*, volume: 15, number: 3 (August), pp. 298-317.
DOI: *10.58346/JISIS.2025.I3.021*

*Corresponding author: Assistant Professor, Department of ISE, BMS Institute of Technology and Management, Bengaluru, India.

principles that amplify networks and financial systems. This study will be part of the overall process of improving the cybersecurity condition and resilience of financial technologies to more complex and varied vectors of cyber threats.

**Keywords:** Wireless Connectivity, Financial Services, Security Framework, Encryption, Authentication, Cybersecurity, Intrusion Detection.

# 1 Introduction

## 1.1 Definition of Secure Wireless Connectivity Frameworks

The term secure wireless system describes a set of protocols, technologies, and architectural elements that aim to ensure the security of data transfer through wireless networks. These systems have security features that are enabled, encrypted, authenticated, and include secure routing protocols. They also feature threat protection mechanisms to address vulnerabilities, cyber threats, and unauthorized access. Secure wireless systems are intended to ensure secrecy, integrity and availability of information across wireless communication networks, especially across the Wi-Fi, LTE and 5G wireless communications. Compared with wired networks, wireless networks have a higher risk of eavesdropping, spoofing, and man-in-the-middle attacks because the transmission medium is vulnerable; thus, a sound security system is necessary.

## 1.2 Importance of Secure Wireless Connectivity for Financial Internet Services

Mehrban et al., (2020) emphasized the growing threat of cyber intrusions in the financial industry. Convenient mobile services, such as Internet banking, online payment applications, stock trading platforms, and personal finance services, rely on wireless networks, which provide a loophole for cyber criminals. For organizations, one loss of security is considered catastrophic financial loss, significant reputational loss, and serious legal action. As noted in the 2025 economic data breach report, the average cost of a data breach is over $5.9 million, much of which can be attributed to weaknesses in wireless access points. (Charoen & Khern-am-nuai, 2025). Because financial transactions usually involve a real-time transfer of funds as well as sensitive user credentials or private corporate information, protection of wireless channels becomes critical (Udayakumar et al., 2023). At the same time, the introduction of 5G and IoT technologies into bank services increases the risk exposure even further. The use of POS, ATM, and even mobile wallets is based on safe and continuous wireless connections to their backend servers (Almaliki & Al-saidi, 2023). Without any security measures, such connections are vulnerable to cyberattacks (Altaleb & Zoltán, 2023). A watchdog report also notes that the three leading industries responsible for attacking vulnerabilities in the wireless communication environment are financial institutions (Oleiwi, 2022). The development of holistic solutions to wireless security is not only limited to technical requirements but also involves regulation and ethics. Priorities of the wireless payment systems in terms of security can be explained by the use of compliance standards such as PCI-DSS (PCI, 2023), (Maidanov & Fratlin, 2023; Williams & Adamson, 2022).

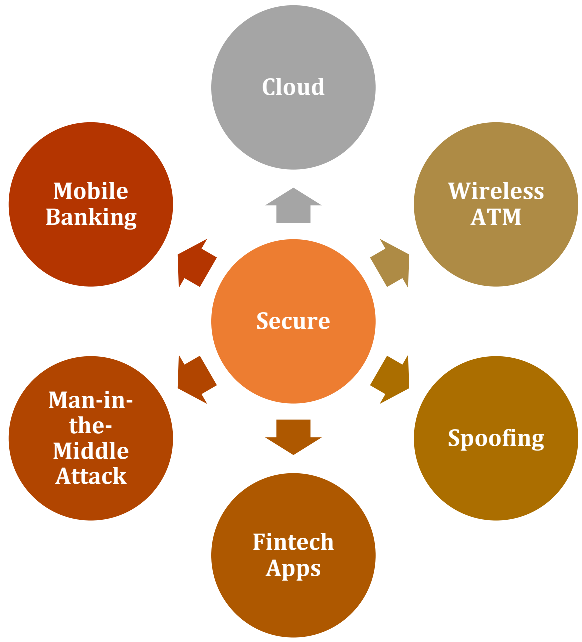


Figure 1(a): Overview of Wireless Connectivity in Financial Internet Services Ecosystem

This figure (Figure 1(a)) illustrates how the wireless connection topography of the global financial system functions, connecting mobile banking, wireless ATMs, cloud services, and fintech applications. The main component of the system is the secure wireless access that links all parts of the financial servicing model to facilitate the transfer of monetary transactions and information. However, the communication link(s) have strata of vulnerabilities that can result in cybersecurity risk events, including man-in-the-middle attacks or identity spoofing and deception, i.e. cyber behavior whereby the expected authenticated user information is stolen and subsequently altered by an attacker. As such, considering numerous cases in recent years, it is clear that strong encryption, protection monitoring and surveillance, and intrusion tracking are required to ensure security, safety, and confidence in wireless financial services.

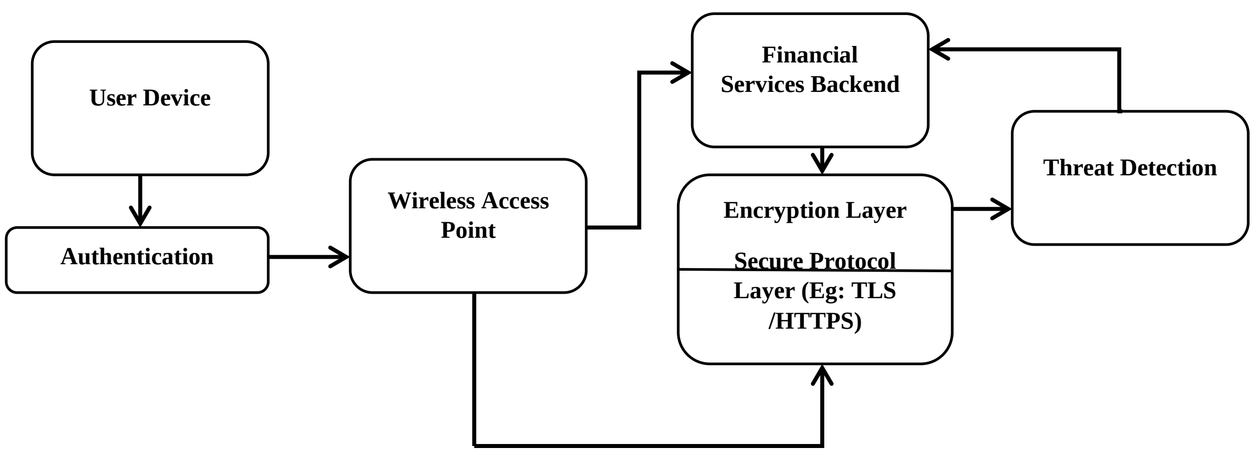


Figure 1(b): Secure Wireless Connectivity Framework for Financial Services

The given illustration (Figure 1(b)) shows a secure and high level architecture of the financial service that uses wireless communication, where the importance is on layered security and data integrity. It begins with a user application on the user device which is authenticated and linked to the financial network via a wireless access point. The protocol layers used in data encryption and protection, such as TLS, HTTPS, and other secure protocols, ensure data confidentiality and integrity by encrypting and securing user communications. As a subsystem generating user transaction, the backend of financial services interacts with other systems dedicated to tracking malicious threat or other suspicious actions. The obtained architecture can improve trust and privacy, making the overall system less vulnerable to cyber threats in wireless financial interactions.

### 1.3 Summary of the Research Document

The present paper explores the application of secure methods for connecting to financial internet services over a secure wireless network. The risk potential networks that could be compromised are Wi-Fi, LTE, 5G, and associated risks have been examined. It was followed by the suggestion of a multi-layered architecture that was secured by end-to-end encryption, VPNs, multifactor authentication and IDPS (Dragomir et al., 2016; Mazhar et al., 2021). Other progressive practices, such as the application of blockchain technologies that provide transparent and verifiable records of transactions, and a zero-trust architecture that demands always-on authentication and limited access, are also presented (Roslan et al., 2024). Exploratory case studies, such as the Capital One data breach and the hack of the SWIFT payment system, are discussed to demonstrate the severe financial implications when wireless security measures are compromised (Ahmad et al., 2021). When considering other PCI-DSS and GDPR security models, the possible reasons for the poor enforcement by financial institutions are discussed. This paper concludes that a wireless access model can be proposed to cut across various segments of financial services. The proposed paper provides a comprehensive overview of ensuring wireless communications in the financial sector by updating the evolution, defining best practices, and specifying relevant legislative frameworks. It attempts to determine the incessant tension of the antagonistic interests of performance, usability, and security, which is required in a modern financial ecosystem (Adejumo & Ogburie, 2025).

This paper will assess the most critical aspects and challenges in achieving secure wireless security in the financial services industry. This study is structured as follows: Section II provides an overview of the various security issues and countermeasures within the fintech services ecosystem currently in operation; Section III delves into more technical details, namely, encryption, authentication, and a secure transmission protocol, among others. Section IV is a series of case studies, which discuss the fact of vulnerabilities being exploited, examples of real-world implementations, and the comparative frameworks between different counterparts; Section V discussion covers larger issues related to new technologies and new regulatory change on an example; and Section VI summarizes the analysis that was done on deficiencies in wireless security in relation to financial institutions and recommends on their improvement of wireless security practices.

## 2 Background

### 2.1 Current Issues in Safeguarding Wireless Connections for Internet Services in Finance

Securing wireless connections in service finance is a complex issue. One of the serious risks is the ability to intercept or snoop on the financial service provider's wireless communication because it is so public. A hacker could easily exploit unprotected Wi-Fi networks or misconfigured cellular networks to capture sensitive transaction information without you knowing (Anisetti et al., 2020). There are also man-in-the-middle (MITM) attacks, which are a common type of aka 'on the wire' sniffing attacks whereby attackers insert themselves between the client user and the financial service to steal credentials and alter the transaction (Bidabad et al., 2017; Verma & Reddy, 2025). The issue of device heterogeneity also raises problems with the implementation of secure wireless financial service. Consumers use smartphones and tablets to access financial services, remote ATMs, and IoT payment terminals, etc. (Shrivastava & Ahmed, 2024). Each of these endpoints has unique security features and vulnerabilities (Mustapha et al., 2023). This heterogeneity among security devices creates difficulties in satisfying a baseline security level across any set of devices. Additionally, the advancement of 5G offers users increased speed and efficiency but also introduces new security challenges, such as social signaling storm attacks and security issues with network slicing (Hartigan, 2024). Ezeh et al., (2024) noted that legacy systems in many organizations are inflexible and cannot support the integration of existing encryption frameworks and authentication processes. Finally, the compliance requirements of GDPR, PCI-DSS, and PSD2 will also be imposed on financial institutions, making it easier to implement security measures.

### 2.2 Review of Literature on Frameworks and Technologies for Ensuring Secure Wireless Connectivity

Several frameworks and technologies have been created to fight threats posed by cybersecurity. End-to-end encryption (E2EE) is one of the initial layers that protects the information between the two data points when the information is being relayed to the receiving endpoint even upon interception. E2EE is in use in mobile banking as well as in payment gateways. Beyond that, Virtual Private Networks (VPNs) are popular for secure remote access and mobile transactions between financial institutions (Ezra et al., 2021), particularly in the context of Bring Your Own Device (BYOD) (Illias et al., 2025). In addition, Multifactor Authentication (MFA) employs multilayered authentication for login, implying that more than one credential is produced to ensure that an individual attempting to log in is who they claim to be. One of the new cybersecurity practices that implements the ideology of never trust, always verify is the Zero Trust Architecture (ZTA). ZTA states that authentication, authorization, and encryption should be done to requests regardless of their origin (Nahar et al., 2024; Assegid & Ketema, 2023). Financial institutions are also ensuring wireless transactions become more secure and transparent by using blockchain technologies, which provide incontrovertible lists of information (Selvam & Stalin, 2018). New wireless security is emerging to incorporate WPA3, TLS 1.3 and 802.1X authentication (Cashel et al., 1997). Such procedures enhance cryptographic security and ban brute force attacks. Moreover, an IDPS has extra protection to wireless networks, as it actively monitors and reacts to malicious actions (John et al., 2024).

### 2.3 An Overview of the Financial Internet Services Landscape

The financial internet services environment refers to the extensive range of multifaceted digital services and platforms that exist in the wireless space. As an example, mobile banking, online trading platforms, peer-to-peer lending apps and cryptocurrency trading platforms, to mention (Ahangaran & Mollakarimi, 2014; Zou et al., 2016). FinTech has contributed with an enormous velocity to the creation of innovative financial products based on mobile-first (Chishti & Barberis, 2016; AlBenJasim et al., 2024). There has been a global increase in digital transactions alongside the prevalence of contactless payment methods and real-time banking services. The World Bank reports that more than 60% of financial transactions in emerging markets are now conducted through mobile wireless platforms (World Bank, 2023; Chitra & Subashini, 2013). The development of Open Banking APIs has further facilitated wireless communication of third-party applications with the banking infrastructure, thereby promoting interoperability, but also expanding the area vulnerable to attacks (Kellezi et al., 2021; Singh & Gurudiwan, 2024). As a result, financial institutions have invested heavily in securing mobile systems and using sophisticated artificial intelligence for monitoring and detecting mobile application vulnerabilities. Nonetheless, the financial services industry remains the most attacked industry because of the great value that data and resources exchanged over wireless networks can bring.

# 3 Secure Wireless Connectivity Frameworks

### 3.1 Encryption Techniques for Securing Wireless Connections

The encryption of information is essential for the wireless transmission of financial information. Encryption transforms human-readable information, or plaintext, into non-human-readable ciphertext, depending on an algorithm and one or more keys. Thus, even if someone intercepts the encrypted data, they are unable to understand any of it. There are two techniques of encryption: symmetric encryption, which uses the same key to encrypt and decrypt the information (AES is one type), and asymmetric encryption, which requires a signed and verified set of public and private keys (for example, RSA). For data transmission to bulk encrypt large data sets, symmetric encryption is preferred due to its speed. In contrast, asymmetric encryption is typically limited to starting the initial handshake or key exchange. Session-based encryption is generally implemented in a wireless environment. Every device generates its own unique key for each session, which HUDDLE believes makes it harder for adversaries to find and exploit an intercepted data packet. Stronger schemes, such as Perfect Forward Secrecy (PFS), built into TLS provide even more protection, as any compromised session key cannot help decrypt previously completed sessions.

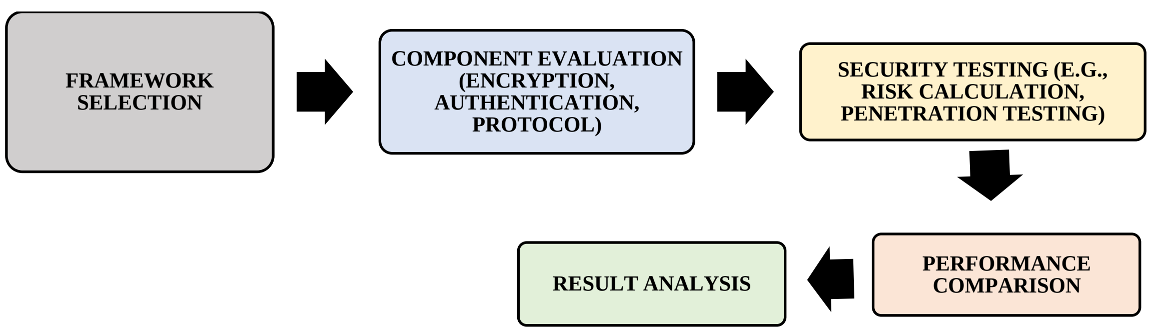


Figure 2: Methodology Workflow for Evaluating Secure Wireless Frameworks in Financial Systems

The graph (Figure 2) presents a process approach to evaluating the security qualities of wireless networks within an economic system, divided into six steps. The first step begins with the selection stage on a security model and then progresses to the component assessment stage, which focuses on encryption, authentication, and communication protocols. Security Testing is followed by risk analysis, and vulnerabilities are tested using pen testing. The results are evaluated based on the performance measures of efficiency and robustness, as identified in previous research. The results of the systematic analysis are compared with the stated goals derived from a rational evaluation. This systematic methodology will guarantee a systematic study of wireless security within economic contexts.

### 3.2 Authentication’s Primary Techniques as Verification of Users’ Identities

Authentication is the process of verifying the identity of financial services users. Multifactor authentication (MFA) is the most extensive security measure that involves a user confirming or authenticating themselves by using at least two out of three types: knowledge (password), possession (mobile device, token), and biometrics (who they are). In addition to that, the contemporary framework comprises of context sensitive multifactor authentication that examines the place, device, and user pattern. In scenarios where there is an inconsistency, for example, a login attempt from a foreign country, the system either requests further confirmation or prevents access to the login functionality. Digital certificates issued within the framework of a public key infrastructure are also standard. For instance, in PKI, wireless devices and users are authenticated based on certificates provided by trusted certificate authorities (CAs). Mobile and web financial applications benefit greatly from authentication-based OAuth 2.0 and OpenID Connect protocols, which allow users to grant application access without sharing their passwords.

### 3.3 Security Procedures for The Supramundane Information Process of Financial Matters

The confidentiality underlying sensitive information on financial transactions is universally based on robust communication methods integrated with encryption and authentication. Wireless communication rules are best achieved by TLS 1.3, which guarantees confidentiality, integrity, and authentication by encrypted handshakes and message authentication code (MAC). Other wireless security protocols are IPsec for securing network layer level communications in a VPN, and HTTPS, which is HTTP over SSL/TLS, thus a secure web communication protocol. Wi-Fi environments at the network access layer are offered dynamic key management and encryption by 802.1X and WPA3-Enterprise. By establishing such protocols, the network will only be accessible to the devices with valid credentials and unauthorized devices will not be able to gain access to the network. In a bid to integrate encryption, authentication with secure protocol transmission in a wireless financial system, we introduce a comprehensive model known as the Triple Layer Secure Wireless Framework (TLSWF) that will ensure a holistic security.

### Proposed Model: Using a Triple Layer Framework for Secure Wireless Connectivity

We suggest a model that integrates three levels of protection namely encryption, authentication, and the transmission of secure data. This model will be defined as Triple Layer Secure Wireless Framework (TLSWF).

Mathematical Representation:

Let:

$D$ represents the data that is going to be transmitted.

$E_k(D)$ represents the encryption of data with a provided key $k$.

$A(u, c)$ represents the authentication function verifying user u with credential $c$.

$P(E_k(D))$ means the transmission of encrypted data will be performed following the established protocol. $if\ A(u, c) = True\quad if\ A(u, c) = True\ \ P\left(E_k(D)\right)$

Thus, the formula for secure transmission $S$ can be expressed as:

$$S = \begin{cases} P\left(E_k(D)\right) if\ A(u,c) = True \\ Access\ Denied\ \ if\ A(u,c) = True \end{cases} \tag{1}$$

This model guarantees that:

Authenticated users $A(u, c)$ are the only ones who can access the data.

All the data is $D$-encrypted $E_k(D)$.

Data communication P is done via a protocol that ensures the confidentiality of the data.

his approach eliminates the odds of man-in-the-middle attacks, user impersonation and unauthorized access to a user using wireless communication, which forms a potent defense mechanism against financial internet facilitation.

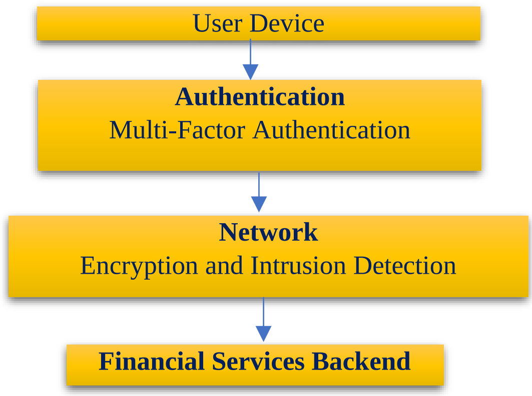


Figure 3: Triple Layer Secure Wireless Framework

Figure 3 shown above is the model of a strong security of communications in financial services industry. It has 4 layers, that is, the User Device, Authentication, Network, and Financial Services Backend with each providing security features, such as Multi-Factor Authentication, Encryption, and Intrusion Detection with layers to provide integrity protection.

**Algorithm for Securing Wireless Connectivity in Financial Services:**

1. **Initialize System**:
    - Set up wireless network infrastructure (Wi-Fi, LTE, 5G).
    - Configure the security protocols (e.g., WPA3, TLS 1.3).
2. **Authentication**:
    - **Step 1**: User attempts to access financial services via wireless network.
    - **Step 2**: Verify user credentials using multifactor authentication (MFA).
    - **Step 3**: If authentication is successful, proceed; else deny access.
3. **Data Encryption**:
    - **Step 1**: Upon successful authentication, initiate end-to-end encryption for data.
    - **Step 2**: Encrypt transaction data using strong encryption algorithms (e.g., AES-256).
    - **Step 3**: Encrypt the user's sensitive data, including credentials, financial transactions, and other confidential information.
4. **Data Transmission**:
    - **Step 1**: Transmit encrypted data over the wireless network using secure protocols (e.g., HTTPS, TLS).
    - **Step 2**: Ensure data integrity through hashing mechanisms to detect any alterations during transmission.
5. **Intrusion Detection**:
    - **Step 1**: Continuously monitor network traffic for suspicious activity using an Intrusion Detection System (IDS).

- Step 2: Flag any anomalies or attacks (e.g., MITM, spoofing, etc.).
- **Step 3**: If a threat is detected, trigger an alert and block the malicious access.

6. **Transaction Completion**:
   - **Step 1**: Once data is securely transmitted and verified, complete the financial transaction.
   - **Step 2**: Record transaction details on a blockchain ledger for transparency and immutability.
7. **Post-Transaction Security**:
   - **Step 1**: Encrypt session data before closure.
   - **Step 2**: Securely log out users and terminate sessions.
   - **Step 3**: Revoke session tokens to prevent session hijacking.

This algorithm outlines an official procedure of achieving wireless connectivity within financial services such as authentication, encryption, data transfer and continuous monitoring of threats.

# 4 Case Studies

## 4.1 Studies on the Secure Wireless Connectivity Framework Implementation in Financial Services Institutions

Some financial institutions have had the experience of deploying secured wireless frameworks with some success. These implementations are multi-tiered security architectures that provide robust encryption, real-time authentication, and mobile banking, ATM, and wireless PoS interfacing control at their corresponding backend.

Some of the implementations may have:

- Full AES-256 encryption
- Two-step biometric or one-time password authentication
- TLS 1.3 for all web and API communications

These protocols cumulatively safeguard the systems and protect them from preemptive or unauthorized breaches on public and open networks. The total effectiveness of the Security (SS) control measures of the security frameworks can be determined using a multiplicative model of prescribed Security (E), trust in the system authentication (A), and assurance of integrity of each invoked protocol (P):

$$SS = E * A * P \tag{2}$$

For instance, if encryption is rated at 0.95, authentication at 0.92, and the protocol's validity at 0.90, then:

$$SS = 0.95 * 0.92 * 0.90 = 0.7866 \tag{3}$$

This indicates a strong security measure effectiveness of 78.66% which is considered strong; however, in situations where detection of behavioral anomaly or adaptive access control is introduced, performance, either hard or soft, can create further enhancements to the overall reliability.

## 4.2 Analysis of Possible Gaps in Standards and Frameworks

There are still many frameworks that can be subject to continual dangerous vulnerability issues, even when observations are made, due to changes in cyber threats and technological practice. Listed below are a number of areas of common concern:

Ineffective session control: If tokens are not properly invalidated or encrypted, attackers may hijack active sessions.

Low device authentication: Many systems rely on Device ID or even Cookies, which can easily be spoofed.

Dependence on outdated protocols: Legacy wireless protocols like WEP or older TLS versions (TLS 1.0 or 1.1) create risk.

Risk exposure (RE) can be calculated based on three individual factors: severity of vulnerability (V), probability of exploiting vulnerability (P), and level of impact (I):

$$RE = V \times P \times I \quad (4)$$

For example, for a framework with vulnerability severity 0.8, likelihood of exploitation at 0.6, and impact value of 0.9:

$$RE = 0.8 \times 0.6 \times 0.9 = 0.432 \quad (5)$$

An exposure to calculated risk at 0.432 indicates there may be moderate to high security risk in the framework and that counteracting measures such as Intrusion Detection Systems (IDS), or regular security patches and updates, are warranted.

### 4.3 Comparison of Various Frameworks' Efficiency in Safeguarding Financial Internet Services

The financial institutions also offer disparate wireless security frameworks that come with different features and strengths. Three of the most common are:

Classic Layered Frameworks: integrate encryption and authentication alongside firewall rule sets.

Zero Trust Architecture (ZTA): Claims no prior trust; therefore, users/devices are verified constantly.

Blockchain-Based Frameworks: utilize distributed ledgers along with smart contracts to verify data.

In this analysis, as an example of the comparison, we can propose a general level of Security Effectiveness Index (SEI) as a weighted sum of primary constituents:

$$SEI = w_1E + w_2A + w_3P \quad (6)$$

Let's define:

$E$ = encryption robustness

$A$ = authentication effectiveness

$P$ = protocol compliance

Also for $w_1, w_2, w_3$ = organizational concern dependent weights with $w_1 + w_2 + w_3 = 1$

Assuming the following ratings:

Framework A (Layered): $E = 0.88, A = 0.85, P = 0.80$

Framework B (ZTA): $E = 0.90, A = 0.92, P = 0.95$

Weights: $w_1 = 0.3, w_2 = 0.4, w_3 = 0.3$

Then:

$$SEI_{\mathbf{A}} = 0.3(0.88) + 0.4(0.85) + 0.3(0.80) = 0.853 \quad (7)$$

$$SEI_B = 0.3(0.90) + 0.4(0.92) + 0.3(0.95) = 0.922 \quad (8)$$

The advantages offered by Framework B's protection are superior, particularly in areas where threat elements are very dynamic and fluid.

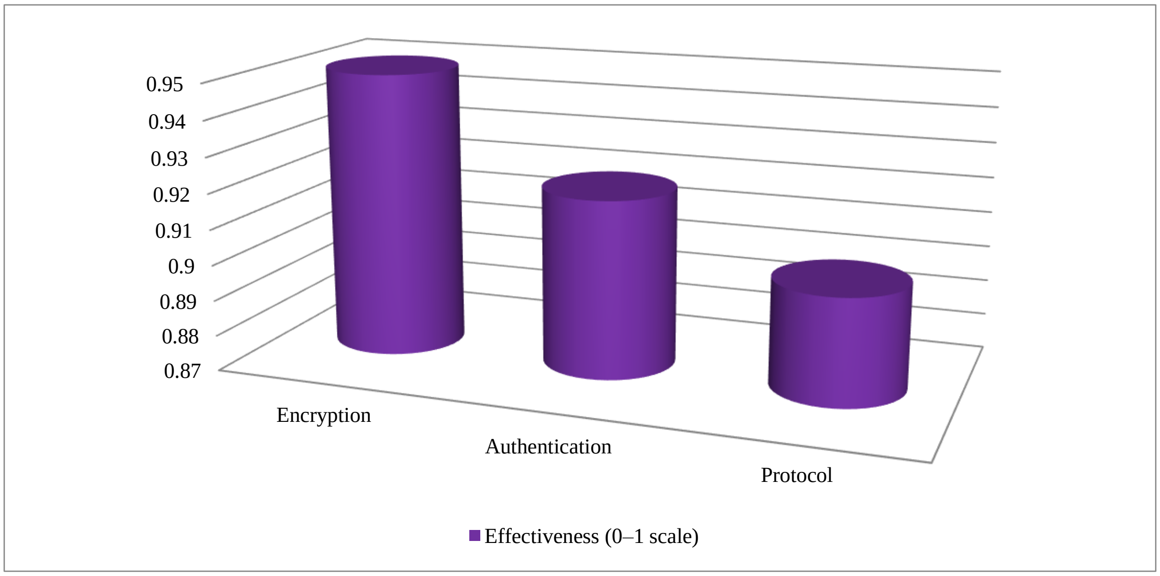


Figure 4: Security Strength Across Components in a Successful Framework

Figure 4 represents the contributions to overall security strength of the various components of the security model-Encryption Strength, Authentication Effectiveness, and Protocol Compliance, as an overall deck security strength to a successful wireless framework in financial services. The effectiveness of each component is relative as summarized across its overall grading component scale factor dimension. While the Encryption Strength component provides a greater contribution to total security strength than the other three in the hierarchy of the need to consider secure financial transactions, that is not to infer that the different components are not consequential.

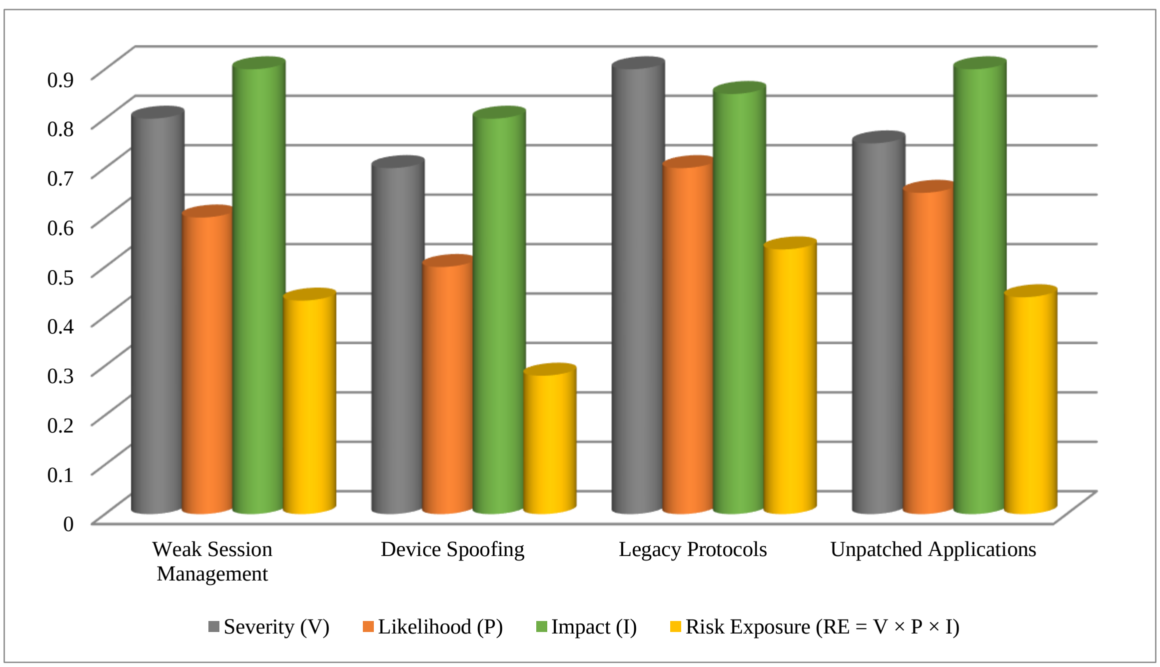


Figure 5: Risk Exposure for Different Vulnerabilities

This graph (Figure 5) is concerned with the contributions of three components: encryption, authentication, and secure protocol for wireless communication of a financial institution. Each element contributes to the strength of security that a financial institution's wireless connection incorporates. The highest score was with encryption effectiveness 0.95 that demonstrates trust in security ciphers like AES-256. Authentication followed at a score of 0.92, establishing confidence in biometric and two-factor authentication. The three remaining components Protocol Robustness was in the center at 0.90 indicating good protocols using TLS 1.3 for example. The value of encryption effectiveness, authentication and protocol robustness were all close together representing a more balanced mitigation approach where one component was not significantly worse than the other. This provides emphasis of how effective multilayer security mechanisms are in thwarting compromise of the system. The graph (Figure 5) depicts the risk associated with the four common vulnerabilities in wireless financial services - weak session management, device spoofing, unpatched applications, and legacy protocols. The graph demonstrates the severity, likelihood, and impact of each of the four vulnerabilities, providing a single risk value. The risk associated with legacy protocols, which involved encryption and compatibility issues, resulted in a risk exposure of over 0.5355. Unpatched applications were just behind that vulnerability with an associated risk value of 0.432, and weak session management was a close risk value of 0.43875. The most alarming vulnerability of BYOD systems is device spoofing, although the value of exposure is also high 0.280. The graphs show that the institutions must pay attention to the enhancement of their security posture in the risk areas.

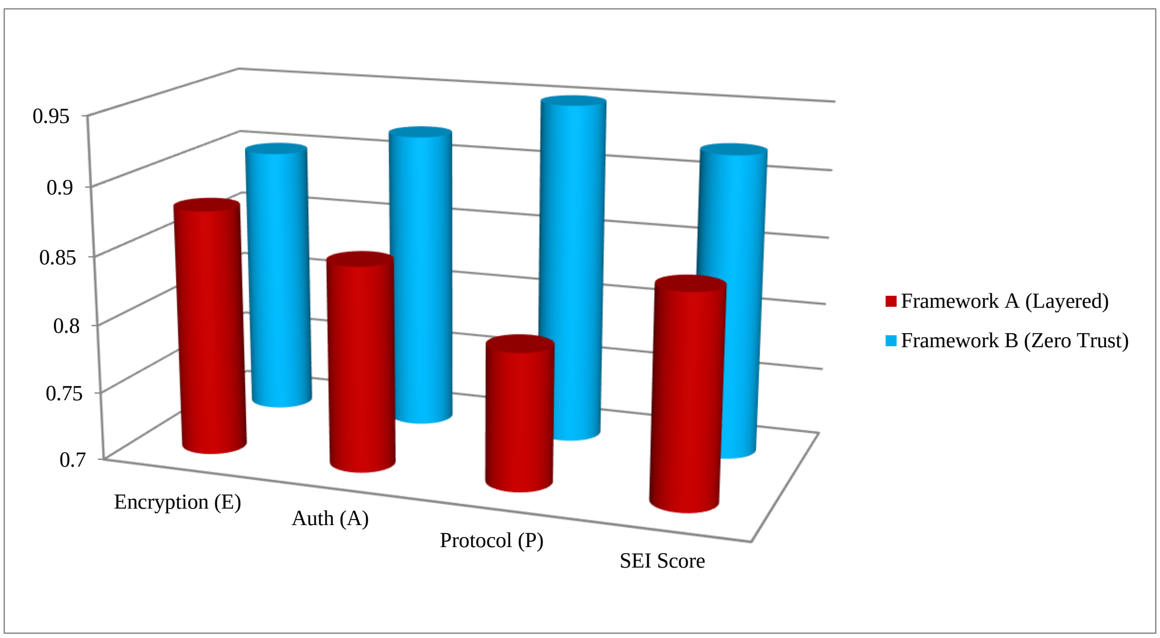


Figure 6: Framework Comparison Based on Security Effectiveness Index (SEI)

Figure 6 compares the scores of two commonly used security frameworks, namely, Layered Security (Framework A) and Zero Trust Architecture (Framework B), regarding the encryption, authentication, and protocol strength. Framework B scored consistently higher in all domains: 0.90 in encryption, 0.92 in authentication, and 0.95 in protocol strength. In contrast, Framework A scored 0.88, 0.85, and 0.80 in the same areas, respectively. Overall, the Security Effectiveness Index (SEI) calculated from these values was 0.853 for Framework A and 0.922 for Framework B. When ranked appropriately through these scores, this figure proves that Zero Trust approaches are better than traditional layered frameworks for high mobility to secure the financial service wireless environment.

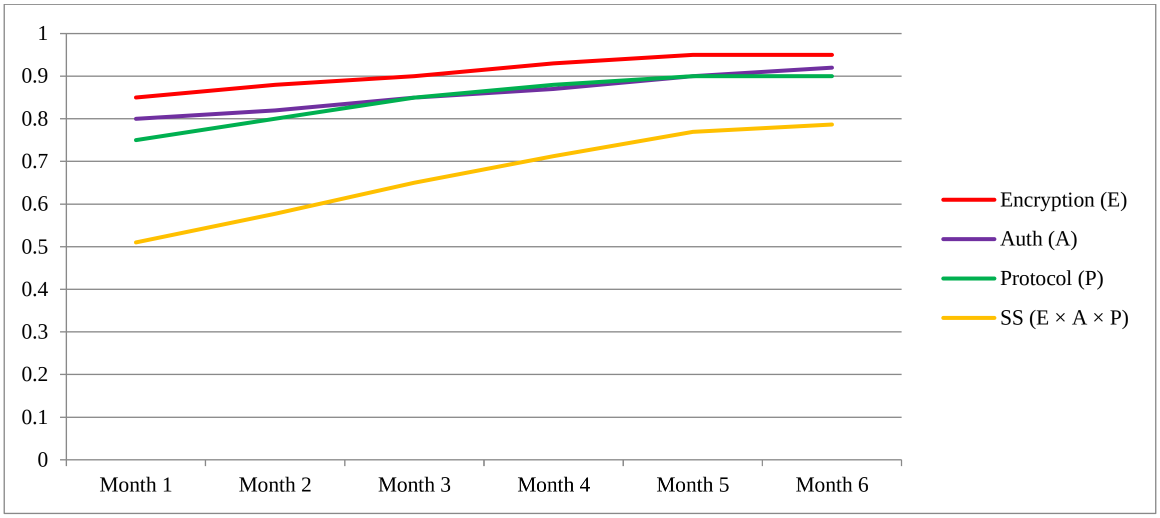


Figure 7: Overall Security Strength Score Over Time (Implementation Phase)

This line graph displaying an evolution (Figure 7) represents the overall security of a wireless environment over a 6 month period. Initially, the encryption, authentication, and protocols provide a starting score of 0.51. During the 6 months of implementation, the organization makes a series of enhancements: utilization of stronger encryption, updates to authentication, and improved protocols. Each series of changes result in predictive trends observable in the results. By month 6 the security has been enhanced to 0.7866. The graph looks at a more maturation and customized implementation process for the organization. The results of the graph are a representation of the improved security due in part to minor enhancements instead of single step enhancements in any spectrum of implementation. It demonstrates the constant evolution of security.

Table 1: Case Studies on Secure Wireless Connectivity in Financial Services

| Case Study | Framework Implemented | Security Measures | Key Findings | Challenges Encountered | Lessons Learned |
|---|---|---|---|---|---|
| **Capital One Data Breach** | Layered Security (AES-256, TLS 1.3) | Multi-Factor Authentication, Encryption, Intrusion Detection | Breach exploited misconfigured firewalls and weak access control. | Lack of proper encryption management and monitoring of access points. | Regular security audits, better monitoring, and incident response plans. |
| **SWIFT Payment System Hack** | Blockchain-Based Security | End-to-End Encryption, Blockchain, MFA | Attackers accessed the system through compromised credentials. | Outdated security protocols and insufficient real-time monitoring. | Adoption of updated protocols, continuous monitoring, and zero-trust models. |
| **Targeted Phishing Attacks in Mobile Banking** | Zero Trust Architecture (ZTA) | Identity Verification, Continuous Authentication | MFA and continuous authentication helped in preventing large-scale fraud. | Slow response time to phishing attacks. | Need for real-time anomaly detection systems and user awareness programs. |
| **Mobile Banking in Emerging Markets** | VPN and Secure Web Communication Protocols (HTTPS) | VPN, TLS 1.3, Mobile Device Authentication | Secured mobile banking applications prevented unauthorized access. | Device compatibility and network instability in remote areas. | Strong encryption, VPN for remote access, and adaptive device compatibility protocols. |
| **ATM Network Breach in 2023** | Advanced Encryption and Intrusion Detection Systems | AES Encryption, IDS, MFA | Attackers exploited weak authentication mechanisms and network vulnerabilities. | Lack of secure communication channels and inadequate real-time monitoring. | Implementing stronger authentication mechanisms and encryption at every communication layer. |

The table 1 outlines key case studies in the financial services of secure wireless frameworks. The summaries, in each of the case studies, encompass the framework(s) applied, security controls in place, highlights of the results, challenges in implementing, and what was learnt. It is a structured format which can give a simpler view of real challenges and solutions in terms of ensuring a system of accessing wireless financial services.

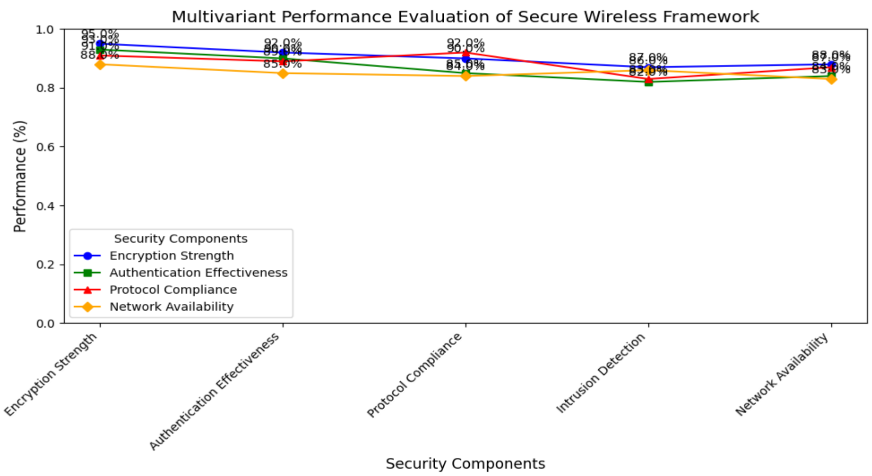


Figure 8: Multivariate Performance Evaluation of Secure Wireless Framework

Figure 8 above examines the main security elements of a secure wireless infrastructure of financial services. It uses a multivariate approach to collect and compare the strength of encryption, effectiveness of authentication, compliance with protocols, and availability of the network. The graph provides the contribution of each component in relation to the overall performance in security with each of the performance values being expressed as a percentage. The effectiveness of each element is reported as a line between every data point and this line shows the effectiveness of the entire security components in safeguarding financial interchange in a wireless network.

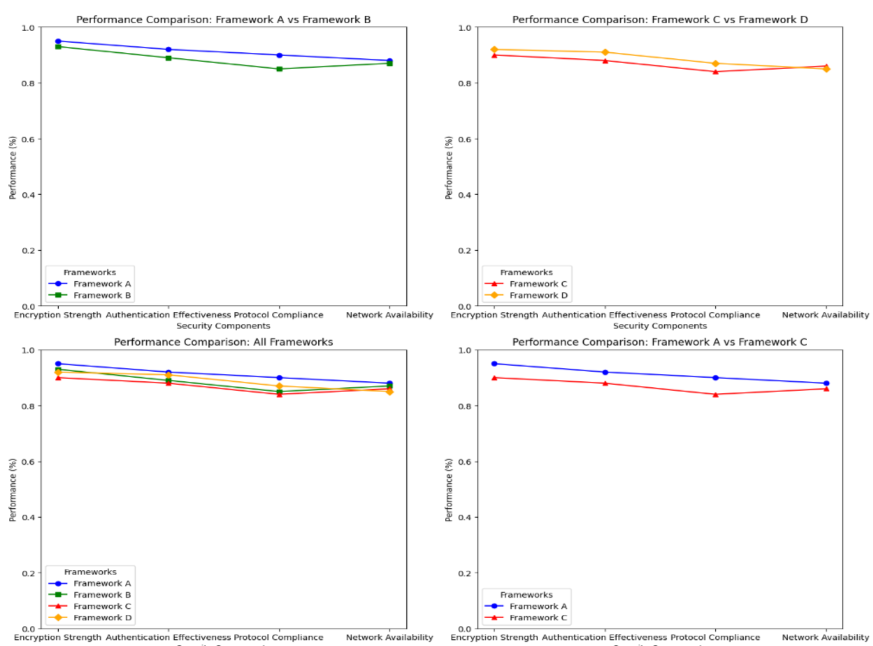


Figure 9: Performance Comparison of Security Frameworks in Wireless Financial Systems

In figure 9, The capabilities of the four security frameworks (Frameworks A, B, C and D) are discussed using the essential security components (Encryption Strength, Authentication Effectiveness, Protocol Compliance and Network Availability). The multivariant graphs provide an outline of the manner in which different frameworks are applied to achieve security of the wireless communications within the financial environment, and give some insight on the weaknesses and strengths of the frameworks. The comparison comes in handy when establishing the most appropriate steps to secure the critical financial activities within a wireless environment.

Table 2: Performance Comparison of Security Frameworks in Wireless Financial Systems

| Security Component | Framework A | Framework B | Framework C | Framework D |
|---|---|---|---|---|
| **Encryption Strength** | 95% | 93% | 90% | 92% |
| **Authentication Effectiveness** | 92% | 89% | 88% | 91% |
| **Protocol Compliance** | 90% | 85% | 84% | 87% |
| **Network Availability** | 88% | 87% | 86% | 85% |

This table 2 presents a performance comparison of 4 security frameworks (A, B, C, D) against four relevant security metrics that apply to the wireless financial systems environment. The metrics included in this comparison are Encryption Strength, Authentication Effectiveness, Protocol Compliance, and Network Availability. For each of the frameworks, the performance is reported as a percentage value to quantify the degree to which each framework achieves security for wireless transactions in a financial context. While the performace comparison percentages in the table are similar to the performance comparison graphs presented in a qualitative way, the table provides a numerical synthesis.

# 5 Future Trends

## 5.1 New Technologies for the Improvement of Security Related to Wireless Connections in Internet Finance Services

Technological advancements like quantum computers pose a threat to RSA and ECC bonds that cannot be secured using older encryption techniques. However, there are new technologies that would enable secure wireless connections in financial services by using encryption algorithms that are resistant to a quantum computer attacking the same connection integrity. Once quantum computers are applied, advanced means of protecting the security of data transmission in wireless channels may utilize lattice-based and multivariate encryption. The use of artificial intelligence in the detection of security threats is also a paradigm shift that utilizes a new system that looks for patterns in network traffic that an AI analyzes as the system looks for changes in the system. Anomaly detection and keeping suspicious activity in check will also happen all at once by AI without any human intervention supporting secure systems known as adaptive security that can self-manage security in response to fluctuating levels of danger. Embedded cryptography bolsters security structures for wireless operations, while updated G5 and Wi-Fi 6 technologies enable less latency and advanced bandwidth. Rather than relying on a single sourced server that can be easily fault crashed, new blockchain based identity managers are helping to lessen reliance on this protection for changes to identity based management. Finally, edge compute tech is being used to complete sensitive tasks closer to the data source and lessen exposures within network operations. This methodology is being used for everything from mobile banking to contactless payments and wireless ATMs.

### 5.2 Possible Changes to Policies Impacting Wireless Connectivity Frameworks

With increasing sophistication in cyber attacks, it is likely that governments and regulators will increase compliance governance on wireless communications and finance. One consideration for policymakers may lead towards standard-setting encryption requirements for financial services institutions. A standard-setting encryption requirement will likely be interpreted by that institution as requiring TLS 1.3 or a more robust encryption protocol, and that would serve the bare minimal requirement for having coherence in systems that engage with one another in financial systems. Policies will also escalate for organizations in processing mobile transactions at scale requiring they implement a zero trust architecture (ZTA). ZTA frameworks require that whoever is requesting access to data, whether via internal or external, has that access verified, which will provide increased control of access. Another example of policy compliance future outcome is regulatory overhaul of requiring data localization, where an institution has regulation if they are required to keep transactional data within the borders of that country, this could have implications on sourcing and laying out their wireless connectivity. This may require the incorporation of secure local edge servers or purpose-built data routing systems. Additionally, regulators may require regular independent evaluations of the security of the wireless system and the operational controls for mitigating vulnerabilities, using third-party experts in the security posture of the framework and work towards timely remediation of identified vulnerabilities. These evaluations may become a requirement for maintaining a banking-credentials or cyber security credential mark through some form of license or certification. The end result for these types of changes is that compliance will need to be built into the architecture of the system, not as an addition at the end and it will require some agility from the financial institutions.

### 5.3 Suggestions on Enhancing Security in Financial Internet Services Accessible through Wireless Connections

Financial institutions should install different technologies and policies, as well as training paradigms to enhance their security measures. Primarily organizations must adopt a defense-in-depth strategy with high encryption, multifactor authentication, secure protocol, meaningful monitoring among other relevant requirements within the security of the cybersecurity baseline in the industry. These organizations should expand their detection capabilities of a systems failure, which can be accomplished by trying to make the network of institution experience immediate investigation analytics for liability reduction. The implementation of the Security Information Event Management (SIEM) achieves extensive wireless detection. Utilizing device attestation and behavioral analytics of a user applying trusted user and trusted device reduce the probability of insider and spoofing attacks. On the other hand, securing the outer boundaries and carrying out consistent penetration testing and simulations-focused cyberattacks against the institution's wireless networks advances security. By possessing a plan to improve defenses within the wireless environments prior to being discovered by real attackers; this is an attempt to address the training gap that will be difficult to close. By constantly reiterating Stephanie's strategy against phishing and credential theft education, end-users are the first line of defense against the misuse of wireless systems. By attempting to prepare for changes in technology and regulations being implemented, financial institutions prevent, protect, and maintain compliance within their operations while improving users wireless access to the institutions infrastructure.

# 6 Conclusion

As previously noted in this research project focusing on protective architectures for wireless access in financial internet services, cybersecurity and technological development are increasingly intertwined. As professional and average users become more accustomed to depending on experiences like mobile banking and contactless payments rely on these systems, security has become paramount. Some of this study's take-aways include the user experience associated with security-in-depth approaches measuring efficacy, growing threats due to legacy policies, and improved infrastructures like Zero Trust to protect critical financial information. With the use of new supports like quantum resistant encryption, AI algorithms to detect threats autonomously and high-level 5G wireless, the use of which will be applied to componentize dynamic operational efficiency, financial security in the field of wireless will further develop to the future with a formidable defensive line. These solutions, however, should grow compliant with the law under the condition of real-time surveillance, encryption being mandatory and safeguarding of sovereignty of information. In the case of banks, and other financial institutions, this signals the beginning of a trend in more compliance-oriented policies which are proactive, via adaptive, anticipative security policies and measures. This must mean that the financial sector redefine their perception of wireless security as not a defensive mechanism but an investment, developing resilience, trust and innovation in the wireless digital finance infrastructures will put the 21st century of finance in a trust space. Besides, to sustain the global finance integrated and supported as it moves forward in both the payment transaction and in the security echoes, organizations will have to embark on establishing networks that further build their trust and reputational safety.

# References

[1] Adejumo, A., & Ogburie, C. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), 1527-1541.

[2] Ahangaran, M. R., & Mollakarimi, F. (2014). The Jurisprudential and Legal Analysis of the Delayed Payment Fine in Banking Contracts in Iran. *Journal of Shi'a Islamic Studies*, *7*(1), 37-63.

[3] Ahmad, A., Maynard, S. B., Motahhir, S., & Anderson, A. (2021). Case-based learning in the management practice of information security: an innovative pedagogical instrument. *Personal and Ubiquitous Computing*, *25*(5), 853-877.

[4] AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, *64*(6), 835-851.

[5] Almaliki, O. J., & Al-saedi, M. O. (2023). The Impact of the Qualitative Peculiarities of Accounting Information Based on the Financial Reports of Commercial Banks. *International Academic Journal of Social Sciences*, *10*(1), 49-56.

[6] Altaleb, H., & Zoltán, R. (2023, July). Addressing cybersecurity challenges in 5G-enabled IoT and critical infrastructures: a comprehensive overview. In *2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES)* (pp. 000131-000136). IEEE.

[7] Anisetti, M., Ardagna, C., Cremonini, M., Damiani, E., Sessa, J., & Costa, L. (2020). Security threat landscape. *White Paper Security Threats*.

[8] Assegid, W., & Ketema, G. (2023). Assessing the Effects of Climate Change on Aquatic Ecosystems. *Aquatic Ecosystems and Environmental Frontiers*, *1*(1), 6-10.

[9] Bidabad, B., Abdollahi, S., & Sherafati, M. (2017). Enforcement of the purports of binding banking documents in Rastin Banking–part I. *International Journal of Law and Management*, *59*(1), 52-65.

[10] Cashel, T. W., McNevin, V. J., Bronson, G., Doggett, J., & Schmelzer, M. J. (1997). Financial Services: Security, Privacy, and Encryption. *BUJ Sci. & Tech. L.*, *3*, 99.

[11] Charoen, D., & Khern-am-nuai, W. (2025). Revisiting the (disappearing) cost of data breach disclosures. *Digital Policy, Regulation and Governance*, *27*(1), 37-55.

[12] Chishti, S., & Barberis, J. (2016). *The Fintech book: The financial technology handbook for investors, entrepreneurs and visionaries*. John Wiley & Sons.

[13] Chitra, K., & Subashini, B. (2013). Data mining techniques and its applications in banking sector. *International Journal of Emerging Technology and Advanced Engineering*, *3*(8), 219-226.

[14] Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016, September). A survey on secure communication protocols for IoT systems. In *2016 international workshop on Secure Internet of Things (SIoT)* (pp. 47-62). IEEE.

[15] Ezeh, F. S., Adanigbo, O. S., Ugbaja, U. S., Lawal, C. I., & Friday, S. C. (2024). Systematic review of digital transformation strategies in legacy banking and payments infrastructure. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 1870-1877.

[16] Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2021). Secured communication using virtual private network (VPN). *Cyber security and digital forensics: proceedings of ICCSDF 2021*, 309-319.

[17] Hartigan, P. (2024). Advancement of Dose Efficacy in Pharmacogenomics with Clinical Practice. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(2), 1-10.

[18] Ilias, I. S. C., Sameon, S. S., Zulkifli, M. Z. E., & Salleh, M. Z. M. (2025, January). Optimizing VPN Security in Financial Services: Implementing 256-Bit Encryption and Tunneling Protocols for Secure Data Transmission. In *2025 19th International Conference on Ubiquitous Information Management and Communication (IMCOM)* (pp. 1-6). IEEE. https://doi.org/10.1109/IMCOM64595.2025.10857544

[19] John, B., Rana, N. S., Nijhawan, M., & Sharma, G. (2024). Developing a framework for ecosystem-based fisheries management in India. *International Journal of Aquatic Research and Environmental Studies*, *4*, 64-70.

[20] Kellezi, D., Boegelund, C., & Meng, W. (2021). Securing Open Banking with Model-View-Controller Architecture and OWASP. *Wireless communications and mobile computing*, *2021*(1), 8028073. https://doi.org/10.1155/2021/8028073

[21] Maidanov, K., & Fratlin, H. (2023). Antennas and Propagation of Waves Connecting the World Wirelessly. *National Journal of Antennas and Propagation*, *5*(1), 1-5.

[22] Mazhar, N., Salleh, R., Zeeshan, M., Hameed, M. M., & Khan, N. (2021, October). R-IDPS: Real time SDN based IDPS system for IoT security. In *2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)* (pp. 71-76). IEEE.

[23] Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., ... & Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, *8*, 23391-23406.

[24] Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B. A., & Yusof, S. H. B. (2023). Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem. *International Journal of Interactive Mobile Technologies*, *17*(22), 100–116. https://doi.org/10.3991/ijim.v17i22.45261

[25] Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6G networks. *IEEE access*.

[26] Oleiwi, A. A. (2022). The Impact of Financial Technology on Promoting the Financial Inclusion of Banks in Arab Countries. *International Academic Journal of Economics*, *9*(2), 39-48.

[27] Roslan, N. I., Mazman, N. T., & Johari, N. F. A. (2024). Zero Trust Architecture: A Paradigm Shift in Network Security.

[28] Selvam, P., & Stalin, N. (2018). Power Transfer Efficiency Analysis of Double Intermediate-Resonator for Wireless Power Transfer. *International Journal of Advances in Engineering and Emerging Technology*, *9*(3), 130-141.

[29] Shrivastava, V., & Ahmed, M. (2024). The Function of the Blockchain System in Enhancing Financial Integrity and the Confidence of Society. *Global Perspectives in Management*, *2*(4), 36-45.

[30] Singh, C., & Gurudiwan, P. (2024). Design and Modeling of Sustainable Environment in Pharmacy and Pharmaceutical Practices. *Natural and Engineering Sciences*, *9*(2), 449-459.

[31] Udayakumar, R., Chowdary, P. B. K., Devi, T., & Sugumar, R. (2023). Integrated SVM-FFNN for fraud detection in banking financial transactions. *Journal of Internet Services and Information Security*, *13*(3), 12-25.

[32] Verma, N., & Reddy, A. (2025). The Demographic Consequences of Urbanization: A Study of Changes in Family Structure and Household Composition. *Progression Journal of Human Demography and Anthropology*, 1-7.

[33] Williams, B., & Adamson, J. (2022). *PCI Compliance: Understand and implement adequate PCI data security standard compliance*. CRC Press.

[34] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727-1765.

## Authors Biography

**Dr.K. Vinutha** Obtained her Bachelor's Degree in Engineering from Channabasaveshwara Institute of Technology, Tumkur. Subsequently, She Completed her Master's Degree in Computer Science and Engineering from AMC Engineering College and Completed her Doctor of Philosophy (Ph.D.) in CSE from VTU, Belagavi In 2023. With a remarkable Teaching Experience, She is actively involved In Research, specifically focusing on Prediction models using Machine Learning Techniques. She has published more than 15 Publications in reputed International Journals and Conferences and delivered 10 Invited Talks in the area of Machine Learning, RPA etc. Her Keen areas of interest encompass Machine Learning and Data Mining. She is a dedicated Life Member of the "Indian Science Congress Association".

**Sivaprasad Lebaka** working as an Assistant Professor in the Electronics and Communication Engineering Department at the Koneru Lakshmaiah Education Foundation located in Vaddeswaram, Guntur District, Andhra Pradesh. He has 14 years of teaching experience and completed his PhD in Electronics and Communication Engineering from VTU, Belagavi, India. He is specialized in leveraging Machine Learning techniques for Image Processing applications. Throughout her academic career, he has contributed 14 papers to international journals in his field of expertise. He is an active life member of the Indian Society for Technical Education (ISTE), Institution of Electronics and Telecommunication Engineers (IETE) and holds memberships in International Association of Engineers (IAENG) and the International Association of Computer Science and Information Technology (IACSIT). Additionally, he has participated in numerous training sessions and conferences that focus on advancements in signal and image processing.

**Capt. Mani Rajakumar is** currently working as Associate Professor at AMET Institute of Science and Technology. He began his maritime career as a Deck Cadet in the first batch of DNS launched by AMET in collaboration with MAERSK and Singapore Polytechnic. He sailed with Maersk Line for 10 years, later serving with Mitsui OSK Lines and as Senior Officer with Farstad Shipping Singapore. His shore-based experience includes worked with Pacific International Lines and Samsara Shipping, managing container operations across major and minor ports around Chennai. He joined AMET as an Assistant Professor in 2010 and has since taught across AMET University, AMET City College and AMET Institute of Science and Technology. He delivers training for BSc, DNS, Pre-Sea modular and simulator-based post-sea modules like ECDIS, ROSC, and ARPA. With rich industry experience and a passion for maritime training, Capt. Mani Rajakumar continues to inspire and guide the next generation of seafarers.

**Dr. Zaid Ajzan Alsalami** is a faculty member at The Islamic University, Najaf, Iraq, in the Department of Computer Techniques Engineering. His research focuses on computer systems, embedded technologies, and intelligent computing applications. He has contributed to research projects and studies aimed at advancing automation, computational methods, and modern engineering solutions.

**Siroj Zarina Rustambekovna** holds a PhD and serves in the Department of Banking and Finance at the *University of Tashkent for Applied Sciences*, Uzbekistan. Her research lies at the intersection of finance and information technology, with a focus on secure digital infrastructures. She has contributed to advancing knowledge on *secure wireless connectivity frameworks for financial Internet services*, highlighting methods to ensure safety, reliability, and efficiency in digital financial transactions.

**D. Dhanasekaran**, an accomplished Assistant Professor and in Electronics and Communication Engineering (ECE), holds a distinguished academic background, having earned his Bachelor's degree from K.S. Rangasamy College of Technology and a Master's degree from Mahendra Engineering College in 2014. Currently doing PhD in authentication protocol in embedded integrated electronics domain. His affiliation with the Indian Society for Technical Education (ISTE) since 2011 underscores his commitment to professional growth and staying updated with industry trends. His dedication to fostering innovation and nurturing talent positions him as a successful mentoring in the field of ECE, driving both academic excellence and practical industry relevance. Throughout his tenure as an Assistant Professor from 2021 to till date and subsequently as a researcher, Mr. Dhanasekaran has consistently exemplified a passion for education and a commitment to student success. Beyond academia, his involvement in mentoring and coaching reflects a dedication to individual growth and development, further cementing his reputation as an influential figure in the field.