International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

Cybersecurity In Fintech Ecosystems: A Systematic Review of Threats and Security Strategies

Vedankita Mohod[1], R.N. Jugele[2]

[1]Assistant Professor, Computer Science, Shri Shivaji Science College, Nagpur, Maharashtra

[2]Professor, Computer Science, Shri Shivaji Science College, Nagpur, Maharashtra

Email id: *vedankitamohod6@gmail.com[1], rn_jugele@yahoo.com[2]*

Abstract

FinTech's tremendous expansion has revolutionized the financial industry by making services like online lending, mobile banking and digital payments possible. Financial systems are becoming more vulnerable to cybersecurity risks, data breaches and financial fraud as a result of this digital transition. Strong cybersecurity has become a significant concern as financial institutions depend more and more on digital infrastructures. The research paper analyses the key vulnerabilities in digital banking systems and addresses the changing cybersecurity issues in FinTech ecosystems. In order to assess current academic research, industry reports and cybersecurity frameworks, the study uses a systematic literature review (SLR) methodology together with exploratory and descriptive research approaches. Important security algorithms utilized in financial transactions, such as AES, RSA, ECC, SHA-25 and SSL/TLS protocols, are also covered. The research found that existing solutions frequently address specific risks or separate security tasks, leading in inadequate protection across interconnected FinTech environments. Key research gaps include a lack of integration of various threat indicators, difficulties in explaining and detecting fraud in real time, interoperability concerns and insufficient integration of technological, organizational and governance-level security measures. Based on these findings, the study demonstrates the importance of an integrated and versatile cybersecurity architecture that includes multi-vector threat monitoring, behavioural analytics, intelligent fraud detection and risk management. Such hybrid method can improve detection capabilities, minimize false positives, boost data protection and increase the cyber resilience, consistency and trustworthiness of FinTech payment and financial service ecosystems.

Keywords: *Cybersecurity; Digital Financial Ecosystems; Financial Technology; FinTech; Multi-Layer Security Frameworks.*

1. Introduction

The global financial environment has seen a considerable transformation due to the fast progress of financial technology or FinTech. The delivery and consumption of financial services have been completely transformed over the last 20 years by digital breakthroughs including cloud computing, artificial intelligence, blockchain technology, mobile applications and big data analytics. Digital payments, mobile banking, peer-to-peer lending, digital wallets, online investing platforms, and real-time transaction processing are just a few of the many services that FinTech platforms currently enable [8]. These technologies have increased financial accessibility, increased operational effectiveness and made it possible for financial institutions to provide clients all over the world quicker and more convenient services [12]. Although these benefits, new cybersecurity issues have also been brought about by the increased

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

use of digital financial systems. The potential attack surface for hackers increases as financial services rely more and more on networked digital infrastructures. Cybercriminals now consider financial data, including transaction logs, authentication credentials and personal information, to be quite valuable. Cybercriminals obtain illegal access to financial systems by taking advantage of flaws in networks, applications and human behaviour. This leads to financial losses, identity theft, data breaches and interference with banking operations. [1][2][14] In the current FinTech environment, traditional security measures that depend on perimeter-based defense are insufficient. The complex ecosystems in which today's financial platform's function include cloud services, open banking APIs, third-party suppliers and international digital networks. Although these linked systems improve operational effectiveness, they also add more vulnerabilities. In order to safeguard vital financial infrastructure, financial institutions must implement sophisticated cybersecurity plans that incorporate technology solutions, risk management frameworks and regulatory compliance method. [6][12] The growing sophistication of cyber-attacks is another crucial component of FinTech security. Attackers increasingly penetrate financial systems using sophisticated methods such supply chain hacks, malware infections, phishing tactics and social engineering assaults. These assaults frequently take advantage of both human and technological flaws, making cybersecurity a complex problem that calls for an all-encompassing protection plan. Financial organizations and cybersecurity experts are investigating several technology solutions to improve security in digital banking systems in response to these concerns. To identify and stop cyberthreats, [13][14] real-time monitoring frameworks, artificial intelligence-based fraud detection systems, encryption techniques and authentication methods are frequently used. [7][10] To improve the resilience of financial infrastructures, regulatory organizations and financial authorities have also implemented governance frameworks and cybersecurity standards. [5][13] It is crucial to thoroughly assess the cybersecurity threats connected to FinTech platforms and determine practical mitigation techniques given the increasing reliance on digital financial systems. The study advances knowledge of digital financial security and emphasizes the significance of creating robust and secure financial ecosystems in the age of digital transformation by offering a thorough analysis of cybersecurity issues and defense in FinTech settings. The purpose of this study is to examine previous research on cybersecurity risks in FinTech ecosystems and examine different security measures that are employed to safeguard financial systems. It covers historical development of FinTech, new business models and frequent hacks that impact financial institutions.

2. Research Methodology

2.1.Data Collection

Primary Data: Primary data refers to original information collected directly from respondents. In this study, primary data can be gathered through structured questionnaires, surveys. It provides valuable insights into real-world cybersecurity threats, fraud detection practices and security mechanisms implemented in banking institutions.

Secondary Data: Gather past information on fraud instances, cybersecurity events and machine learning applications for fraud detection from reliable sources, making sure the data is accurate and relevant.

2.2.Exploratory and Descriptive Approach

Exploratory Research: To study the present state of cybersecurity risks in contemporary banking and the use of different techniques in fraud detection, conduct a thorough analysis of the body of existing literature, industry reports and academic research.

Descriptive research: Outline all of the cybersecurity risks that existing financial organizations must deal with, including their traits, effects and historical development.

2.3.Systematic Literature Review Approach

The results of several peer-reviewed scientific publications, including latest research on machine learning-based fraud detection in banking systems and traditional multi-level cybercrime effect models are summarized in this review study. In order to include insights from AI-driven security frameworks and cybercrime effect assessments, the study uses a Systematic Literature Review (SLR) methodology in conjunction with conceptual analysis. Relevance to cybersecurity in financial systems, methodological

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

rigor, technological contribution and theoretical or practical value were among the selection criteria. This method facilitates the creation of a thorough understanding of cybersecurity issues and solutions in the financial technology ecosystem and permits an organized assessment of the body of available material.

2.4.Algorithmic Models Used in Financial Fraud Detection

Security Algorithms Used in Payment Gateways

Several encryption and network security procedures are used at various stages of the transaction process to guarantee safe payment transactions. Confidentiality, Integrity and Authentication are the goals of the following algorithms.

Following algorithms are used in payment gateways

- AES (Advanced Encryption Standard)
- RSA (Rivest–Shamir–Adleman)
- ECC (Elliptic Curve Cryptography)
- SHA-256 (Secure Hash Algorithm)
- SSL/TSL (Secure Socket Layer/ Transport Security Layer)

Security mechanisms

- AES → confidentiality
- RSA/ECC → secure key exchange/authentication
- SHA-256 → integrity/hash-based verification
- TLS → secure communication

3. History And Evolution of Fintech [8]

FinTech has been emerging for over a decade, with five significant stages which witnessed the introduction of emerging technologies.

3.1.FinTech 1.0 (1866-1967)

Infrastructure including steamships, telegraphs, railroads and global telex networks were developed during the FinTech 1.0 era to support international trade and financial communication. The first transatlantic cable was constructed in 1866 to establish a global network infrastructure. Fedwire was established in 1918 to transfer electronic funds using Telegraph and Morse code, a typewriter was used to verify signatures, dinner cards were introduced in 1950 to make cashless restaurant payments, credit cards were introduced in 1958 to solve the issue of carrying cash and screen-based stock data was introduced in 1960, causing the financial market surge. During this time, a large number of joint-stock, banking and insurance businesses were formed. These advances laid the foundation for FinTech 2.0 and were vital for the first industrial revolution.

3.2.FinTech 2.0 (1967–2008)

The Telex, which took the place of the Telegraph in 1966, the Barclays Bank's installation of automated teller machines (ATM) in 1967 and the UK's Interbank Computer Bureau's introduction of contemporary computerized payment systems and electronic clearing services in 1968 are some of the notable innovations of this FinTech 2.0 era. The first electronic stock market was created in 1971 by the National Association of Securities Dealers Automated Quotations (NASDAQ) and the Society for Worldwide Interbank Financial Telecommunications (SWIFT) was established in 1973 to allow financial institutions to send enormous sums of money across international borders. The 1980s saw both the expansion of electronic banking (e-banking) and the usage of mainframe computers in banks. The development of online consumer banking by Wells Fargo in 1995 and the introduction of contemporary cashless payment system known as "PayPal" in 1998 marked the beginning of the expansion of electronic commerce in the mid-1990s. Additionally, the demand for the FinTech industry changed fundamentally as a result of the 2008 financial crisis.

3.3.FinTech 3.0 (2008–2014)

The financial crisis that occurred in 2008 and the rapid development and use of smartphones caused the public to lose faith in the established banking system, which fundamentally changed the need for FinTech 3.0. Globally, a large number of individuals use cell phones to access financial services and the Internet. In a same vein, it has drawn several new FinTech firms in addition to the established traditional financial institutions that have digitalized banking services and made room for new goods and services. In FinTech 3.0, a number of well-known banks from the FinTech 2.0 era departed and relaunched as startups. The financial industry has been greatly impacted by the introduction of Bitcoin in 2009 and other cryptocurrencies based on blockchain technology, P2P lending/payment platforms[8] in

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

2011, mobile wallets (Google Wallet in 2011 and Apple Pay in 2014), credit scoring, Banking as a Service (BaaS) platforms (Treezor and SolarisBank), RegTech, small-ticket loans, insurance technology (InsurTech), property technology (PropTech), wealth technology (WealthTech) and government technology (GovTech).

3.4.FinTech 3.5 (2014-2017)

The worldwide expansion of electronic banking and how individuals in developing countries access the Internet are explained by the FinTech 3.5 era. It looks at how emerging markets like China and India, who use FinTech the most, failed to develop their physical banking infrastructure. Rather, they quickly embraced cutting-edge technology to offer digital banking services, expanding the FinTech industry. In a similar vein, a number of African nations increased Internet access around this time, extending online banking services across the continent. Some of the most notable FinTech innovations during this time include Alipay in China, Payment banks in India, Indian companies creating financial software similar to Software as a Service 2 (SaaS 2) and M-Pesa mobile money in Africa.

3.5.FinTech 4.0 (2018-to date)

The digitalization and data collection of finance, the dominance of digital banking platforms, and new entrants like Big Techs like Meta, Google, Amazon, Tencent and Alibaba are all part of the FinTech 4.0 age [8]. Big Techs process the massive amounts of data gathered from the many activities on their platforms using sophisticated analytical techniques like artificial intelligence. It also examines how the future of financial services is being shaped by disruptive technologies like blockchain and open banking. The method by which artificial intelligence technologies are fighting card fraud and money laundering, how machine learning changes consumer interactions with banks and insurance companies and how customer behaviour is predicted by dynamically identifying new card fraud tendencies are all noteworthy developments. Virtual and augmented reality, digital banking, digital lending, web-based crowdfunding frameworks, InsurTech, PropTech, customer incentives and regulatory technology are further technologies included in FinTech 4.0. Quick response (QR) code-based payment systems are also developed and implemented by integrated payment providers. Quantum computing capabilities are able to develop security protocols. Nowadays traditional network perimeters are focus on securing user identities and devices. As shown in Table 1 FinTech's Technological Innovation and Novel Security Risks, Figure 1 Phases of FinTech Evolution [8].

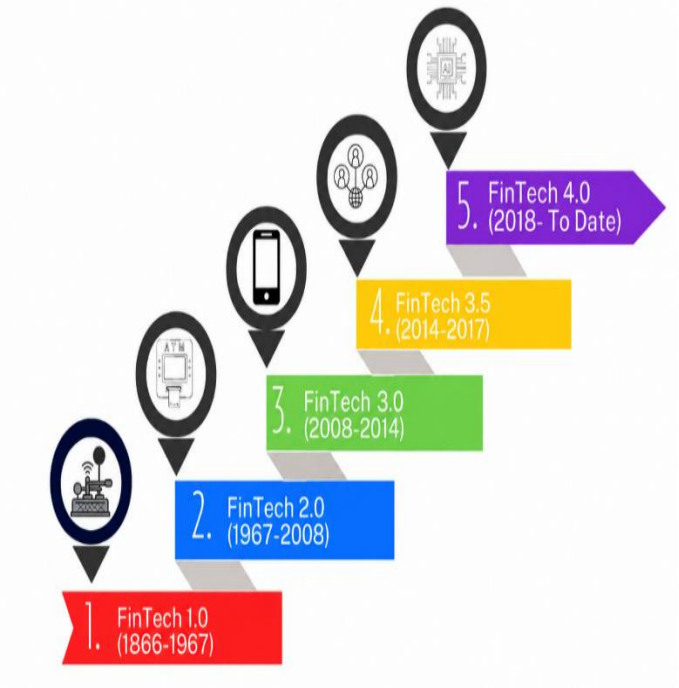

Figure 1 Phases of FinTech Evolution [8]

Table 1 FinTech's Technological Innovation and Novel Security Risks

FinTech Era	Major Technology	Emerging Security Concern
FinTech 1.0	Telegraph/electronic communication	Communication security
FinTech 2.0	ATM/e-banking	Authentication and network security
FinTech 3.0	Smartphones/mobile payments	Mobile fraud and malware

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

FinTech 3.5	Rapid digital adoption	Identity and payment fraud
FinTech 4.0	AI, cloud, APIs, digital platforms	Multi-vector cyber threats

4. Fintech Business Model

4.1.Payment gateway

Customers can pay for goods and services on the retailer's website using these platforms. FinTech firms and businesses give their customers digital wallets and mobile applications so they may swiftly swap and send money for goods and services online, make consumer retail payments, P2P mobile payments, overseas real-time payments and wholesale corporate payments [6]. In order to offer additional functionality, mobile platforms and digital wallets are often linked to other payment systems. Google Wallet, Apple Pay, Alipay, WeChat Pay, PayPal, Stripe, Citi Pay, Venmo, American Express and M-Pesa are some of the well-known digital wallets. They make money through merchant partnerships, transaction fees and exchange fees. These payment options are safe, quick, practical and available through several channels.

4.2.Peer-to-Peer Lending

By connecting borrowers in direct contact with lenders, this internet lending platform eliminates the need for traditional financial intermediaries like banks. In addition to creating loan listings and a decentralized loan marketplace, they employ technology to connect lenders and borrowers, streamline the borrowing and lending process and specify loan amounts, interest rates and expected returns [8]. P2P lending is characterized by online platforms, direct lending, credit evaluation, risk management and openness and disclosure. Prosper Marketplace, Zopa, Funding Circle, Kiva, LendingClub, RateSetter, Peerform, Upstart Holdings and SoFi are some of the top P2P lending platforms. By collecting fees or keeping a portion of the loan, P2P lending generates revenue. They provide a number of advantages, including lower interest rate loans, improved lending procedures for both lenders and borrowers, better returns for investors compared to debt markets, easier access to loans for underprivileged people or small businesses and profitable investment opportunities for money lenders.

4.3.Digital banking

Since the widespread use of mobile devices, Internet penetration and mobile banking applications, which offer a abundance of potent features and services that enable users to monitor their bank accounts, pay bills, deposit money and transfer money directly from their smartphones to and from any location as long as there is an Internet connection, digital banking is widely adopted in the FinTech sector. Among the well-known FinTech banks offering digital banking include PNC Financial Services Group, Narmi, Federal Reserve Bank of Chicago, Leader Bank and FirstBank. They provide a number of advantages, including high security for customers' mobile accounts, ease of use of mobile banking apps, the ability for users to efficiently manage and monitor their financial activities, the need for less human resources and lower transaction rates. The vast majority of digital banks use anti-money laundering technologies and artificial intelligence and machine learning to safeguard against fraud.

4.4.InsurTech

InsurTech startups and well-established companies in the FinTech sector use technology to offer clients cutting-edge insurance services and products more effectively, with a more meaningful the client experience, streamlined healthcare billing processes and more affordable insurance services and products [8]. Artificial intelligence, machine learning, big data, data analytics, blockchain and Internet of Things devices are some of the technologies they use to accurately assess risks, comprehend customer behavior, improve customer service, offer personalized policies, insurance products and services, automate claims processes and help maintain claims more quickly and seamlessly. The widely recognized InsurTech firms upending the insurance sector include Lemonade, Next Insurance, Zego, Hippo, Oscar Health, Policygenius, Acko, Kin Insurance, Root Insurance, Clearcover, GoHealth, Metromile, Coverfox and Bright Health. Both new and established insurtech firms make money by collaborating with insurance carriers and charging

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

premiums. InsurTech solutions help insurers to strengthen their data collection and quickly assess customer data in order to find the best policies, improve risk analysis and make it easier to compare different insurance plans.

5. Common Cybersecurity Attacks

5.1.Social Engineering Attacks

- Phishing: Phishing attacks attempt to extract personal identifiable information through digital means, such as malicious emails that appear to be from legitimate sources and counterfeit websites. More sophisticated scams of this nature tend to account for psychological vulnerabilities in order to manipulate victims, creating a sense of urgency in a way that challenges good judgment. Phishing attacks target the masses striving to reach as many victims as possible. However, spear-phishing is the more focused alternative. A spear-phishing attack can only be executed after initial research and the content of the message is at least tailored to some extent for the individual target [11]. Social networking sites can be used by cyber criminals to mine data on potential victims, extracting information to create extremely customized messages that would appear to be sent by close friends [8][11].
- Spear Phishing: A unique type of phishing assault known as "spear phishing" targets a specific person or group inside a company. Before sending the phishing payloads via a variety of phishing approaches, the attacker tracks and obtains some basic information about the victim. Organizations may suffer financial loss and harm to their brand if these attacks are effective. Because attackers utilize tactics that resemble trustworthy services, spear phishing assaults are very effective and difficult to detect by typical security measures.
- Attackers often target executives and staff, for instance, by sending emails that appear to be from reliable sources and convey a feeling of urgency and significance or they entice the victim to gather sensitive data. Once successfully exploited, the attacker can join the business without authorization and carry out illicit operations including financial frauds, ransomware attacks, malware distribution and the theft and sale of sensitive data on the dark web [11][8].
- Whaling: A sophisticated kind of phishing assault known as "whaling" targets top officials or high-level executives in a business, such as bank managers, CEOs, or CFOs. Whaling attacks target those with more power and access to critical financial or organizational data, in contrast to standard phishing attempts that target a broad number of users. Cybercriminals use meticulously produced emails or letters that seem to be from a reliable source, such a senior executive, regulatory body or business partner, to launch a whaling assault. These messages frequently ask for immediate acts, such authorizing bank transactions, giving private information or transferring money.

5.2.Salami Attacks

A Salami attack is a kind of cyberattack in which financial institution employees or software developers install malware on FinTech servers in order to fraudulently steal a small sum of money from each FinTech client's account and deposit it into another account that has been opened under a different name and is owned by the software developers or employee without the victims' knowledge. A salami attack can have serious repercussions for FinTech businesses and clients as it aims to steal a modest sum of money from each client over an extended period of time without being discovered. Inadequate expenditures from each client can total a sizable sum of money and could lead to significant losses. Due to the little amount deducted, the majority of victims of salami attacks typically do not disclose the deductions to the financial institutions [8]. Both internal and external salami assaults are possible. Dissatisfied or internal software developers of FinTech startups who are familiar with the security system of FinTech platforms carry out internal attacks; Former employees or outside developers who have insider knowledge of the FinTech security system attempt to steal from the FinTech's clients carry out external attacks.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

The attackers use mathematical techniques such as rounding to the closest integer while ignoring other decimals and value computations based on two or three decimal places. Without informing the FinTech startup, the remaining portion of the funds is moved into the attacker's account.

5.3.Shoulder Surfing Attacks

A specific type of social engineering attack known as "shoulder surfing" involves an attacker watching a target while they enter private information in order to gather sensitive information. To get information like passwords, PINs, ATM login credentials or bank account information, the attacker may utilize cameras, binoculars or other recording equipment in addition to peering over the victim's shoulder. This assault frequently takes place in public locations where people access their online banking accounts or input PINs for financial transactions, such as ATMs, banks, cafés, airports or congested areas. Shoulder surfing in the context of online banking can result in identity theft, financial fraud and illegal access to bank accounts if hackers are able to get private authentication data.

5.4.Malware Attacks

Malicious software intended to penetrate, harm or get unauthorized access to computer systems, networks or devices is used in malware assaults. Cybercriminals frequently utilize malware in the context of digital banking and financial systems to steal sensitive data, including credit card numbers, banking information, login passwords and authentication information. Unauthorized software downloads, hacked websites, malicious links and contaminated email attachments can all spread malware. Once installed on a machine, it can steal data, record keystrokes, monitor user activities or interfere with regular system functions. Software downloads, hacked apps, malicious websites and infected email attachments are all ways that malware can enter banking systems. After installation, it can keep an eye on user behaviour, record private information or provide hacker’s remote access.

5.5.Types of Malwares

Virus: A virus is a kind of malicious software that affixes itself to legitimate files or programs. When the compromised file is run, it spreads and can lead to data corruption, system harm or illegal access to private data.

Worm: A worm is a type of malware that replicates itself and spreads over computer networks without the need for human intervention. Worms may quickly proliferate within financial networks, slow down systems and use up network capacity.

Trojan Horse (Trojan): The Trojan Horse is malicious software that poses as a trustworthy application. Once installed, it opens a backdoor that lets hackers access the victim's computer, steal confidential data or install other malware.

5.6.Supply Chain Attacks

An assault that targets the software, hardware or service providers that supply components to an organization instead of the company itself is known as a supply chain attack. Attackers can obtain indirect access to the systems and data of the target company by breaching a reliable third-party provider. Supply chain attacks can happen in the context of digital banking and financial institutions when hackers take advantage of weaknesses in third-party software providers, payment processors, cloud service providers or fintech partners linked to the banking infrastructure. Attackers may use inadequate security procedures in third-party services, corrupt vendor systems or implant malicious malware into genuine software updates. The attacker obtains unauthorized access to sensitive data or vital infrastructure when the compromised software or service is incorporated into the bank's systems.

5.7.Effects on Banking Systems

- Unauthorized entry into financial networks
- Data breaches compromising the financial information of customers
- Banking activities are disrupted
- Large-scale cyberattacks that impact several companies

As shown in Table 2 Threats and Protection Framework in Multilayer Cybersecurity FinTech Systems [4][5][6][14]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

Table 2 Threats and Protection Framework in Multilayer Cybersecurity FinTech Systems [4][5][6][14]

Layer	Threat Domain	Protection Mechanisms	Security Outcome	Core Term	Conceptual Meaning in FinTech
Network	DDoS, MITM, intrusion	Secure networks and monitoring systems	Service availability	Cyber Threat	Digital risks targeting FinTech infrastructure
Application	Malware, injection and vulnerabilities	Secure coding, testing and monitoring	System stability	Cybersecurity	Protection of systems and applications
Data	Breaches, leakage and manipulation	Access control and data governance	Data integrity	Data Protection	Safeguarding financial and personal data
API	Token abuse and API exploitation	API security frameworks	Platform reliability	Risk Management	Identification and mitigation of digital risks
Human	Phishing and insider threats	Training and awareness programs	Trust assurance	Digital Trust	User confidence in FinTech platforms
Organization	Process failures and mismanagement	Policies, compliance models	Operational control	Governance	Policy and regulatory control systems
Enterprise	Systemic cyber risks	Strategic security planning	Institutional stability	Cyber Risk Management	Enterprise-level cyber risk control

Conclusion

The concept of peer- digital payments, mobile banking, digital wallets, and online financial platforms are just a few of the ways that FinTech's rapid growth has revolutionized the financial sector and improved accessibility, efficiency and convenience. However, the growing reliance on networked digital infrastructures has also increased the cybersecurity attack surface and made financial ecosystems vulnerable to a variety of constantly

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

changing threats. FinTech cybersecurity risks are complex and comprise network, application, API, data, human and supply-chain layers, as this assessment demonstrates. Phishing, spear-phishing, social engineering, malware, shoulder surfing, salami assaults and supply-chain attacks are among the major risks identified in the literature. Financial losses, illegal access, data breaches, identity theft and disruptions to financial services are all possible outcomes of these dangers. The results also show that current cybersecurity strategies mostly target specific threat categories or discrete security features, leading to disjointed defense systems. Financial data and digital transactions are significantly protected by encryption algorithms, secure communication protocols, authentication methods, risk management frameworks and multi-layer security structures. However, they might not be adequate to handle sophisticated and coordinated cyber threats in contemporary FinTech environments. As a result, the analysis highlights the necessity for research on an integrated security architecture that can instantly correlate transaction behaviour with diverse cybersecurity threat indicators. Future research should focus on to enhance detection accuracy, lower false positives and reinforce the resilience of FinTech payment gateways, future research should concentrate on hybrid multi-vector cybersecurity frameworks that integrate cybersecurity monitoring, behavioural analytics and intelligent fraud detection. As FinTech continues to develop using blockchain, cloud computing, artificial intelligence and other cutting-edge technologies, such integrated methods can help create digital financial ecosystems that are safer, more dependable and sustainable.

References

[1]. Sekhar, C., & Kumar, M. (2023). An overview of cyber security in digital banking sector. East Asian Journal of Multidisciplinary Research, 2(1), 43–52. https://doi.org/10.55927/eajmr.v2i1.1671

[2]. 2. Jain, S., & Sinha, S. (2024). International Journal of Advanced Legal Research Cyber Security threat in the digital banking sector. https://ijalr.in/wp-content/uploads/2024/02/Research-on-Cyber-Security-Threat-in-Digital-Banking-Sector.pdf Volume 11 Issue 6 June 2024.

[3]. Rohit Kalakuntla, Anvesh Babu Vanamala, Ranjith Reddy Kolipyaka. “Cyber Security”. HOLISTICA Vol 10, Issue 2, 2019, pp. 115-128. DOI:10.2478/hjbpa-2019-0020.

[4]. Nish, A., Naumaan, S., & Muir, J. (2020). Enduring cyber threats and emerging challenges to the financial sector. https://assets.carnegieendowment.org/static/files/NishNaumaan_FincyberThreatsChallenges_v3.pdf

[5]. Publication Edit. (2025). Aigerim sydykova: Cybersecurity in financial technologies: Current threats, methods of protecting user data, and ensuring business security. Aigerim Sydykova: Cybersecurity in Financial Technologies: Current Threats, Methods of Protecting User Data, And Ensuring Business Security. https://www.academia.edu/129345701/Aigerim_Sydykova_Cybersecurity_in_Financial_Technologies_Current_Threats_Methods_of_Protecting_User_Data_And_Ensuring_Business_Security

[6]. Nur Hezreen Camelia Bin Kamaruddin, Mohamad Fadli Bin Zolkipli. “The Role of Multi-Factor Authentication in Mitigating Cyber Threats”. Borneo International Journal eISSN 2636-9826; Vol. 7 (4); 2024; 35-42.

[7]. Guma Ali, Maad M. Mijwil, Bosco Apparatus Buruga, Mostafa Abotaleb. “A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech”. https://ijcsm.researchcommons.org/ijcsm/vol5/iss3/12. Vol. 5: Iss. 3, Article 12. e-ISSN: 2788-7421 p-ISSN: 2958-0544

[8]. Breda F, Barbosa H, Morais T. “SOCIAL ENGINEERING AND CYBER SECURITY”

[9]. Olawale Olowu, Ademilola Olowofela Adeleye, Abraham Okandeji Omokanye, Akintayo Micheal Ajayi, Adebayo Olabode Adepoju, Olayinka Mary Omole and Ernest C. Chianumba. “AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity”. https://doi.org/10.30574/gscarr.2024.21.2.04

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5244 - 5253
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0686

18. GSC Advanced Research and Reviews, 2024, 21(02), 227–237.

[10]. Shiv Mohan, Jatin Sharma. "EVOLUTION OF SPEAR-PHISHING ATTACK" Case Studies and How to Prevent. https://www.seqrite.com/documents/en/white-papers/whitepaper-evolution-of-spear-phishing-attack.pdf.

[11]. Omolara Patricia Olaiya, Temitayo Oluwadamilola Adesoga, Adefisayo Ojo, Oluwabusola Dorcas Olagunju, Olajumoke Oluwagbemisola Ajayi and Yusuf Olalekan Adebayo. "Cybersecurity strategies in fintech: safeguarding financial data and assets". E-ISSN: 2582-4597, CODEN (USA): GARRC2, Article DOI: https://doi.org/10.30574/gscarr.2024.20.1.0241

[12]. Choo K-K R. 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security 30(8): 719–731 (DOI: http://dx.doi.org/10.1016/j.cose.2011.08.004).

[13]. Rami Shehab, Abrar s.alismail, Dr. Mohammed Amin Almaiah, Dr. Tayseer Alkhdour, Dr. Belal Mahmoud AlWadi, and Dr. Mahmaod Alrawad. "Assessment of Cybersecurity Risks and threats on Banking and Financial Services". Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 167-190. DOI: 10.58346/JISIS. 2024.I3.010.