International Journal of Social Impact
ISSN: 2455-670X
Volume 10, Issue 3, DIP: 18.02.084/20251003
DOI: 10.25215/2455/1003084
www.ijsi.in | July – September, 2025

International Journal of Social Impact
A Peer Reviewed Journal

Cybersecurity Challenges in Fintech: Ensuring Data Privacy in a Digital Economy

Dr. Amol Kundalik Sathe [1]*, Shelke Karan Navnath [2], Shelke Saloni Santosh [3], Shelke Vaibhavi Vijay [4]

ABSTRACT

The blistering development of financial technology (Fintech) has transformed the financial services of the globe since it makes transactions quicker, more accessible than ever before, and digital in nature. Such expansion has also posed thorny cybersecurity challenges that have compromised the privacy of data and consumer trust. The more financial system is built on cloud computing and mobile platforms, artificial intelligence, as well as blockchain technologies, the more vulnerable cyberattacks, data breaches, and identity theft, are. This article explains the dynamic characteristics of cybersecurity threats in Fintech, and how the data privacy issue is associated with regulatory compliance, technological innovation, and consumer protection. The study identifies the top threats, including phishing, ransomware, insider attacks, and vulnerabilities to third-party integration. It also discusses how regulatory frameworks, such as general data protection regulation (GDPR), payment services directive (PSD2) and emerging national policies can help in establishing data security standards. Further, the paper concentrates on the necessity of incorporating the current defense controls such as encryption, biometric authentication, secure APIs, and real-time anomaly-detection as a measure of resiliency to cyber threats. The research merges the information of both technical and policy scopes, and in the process, places emphasis on the fact that building trust in digital financial ecosystems extends beyond technical security; it also involves enacting an active governance, user awareness, and collaboration among the sector. Lastly, the evidence reveals that the need to grant data privacy in a digital economy is not to be regarded only as a regulatory requirement but also as a strategic reaction to the survival of Fintech and its capacity to maintain consumer confidence.

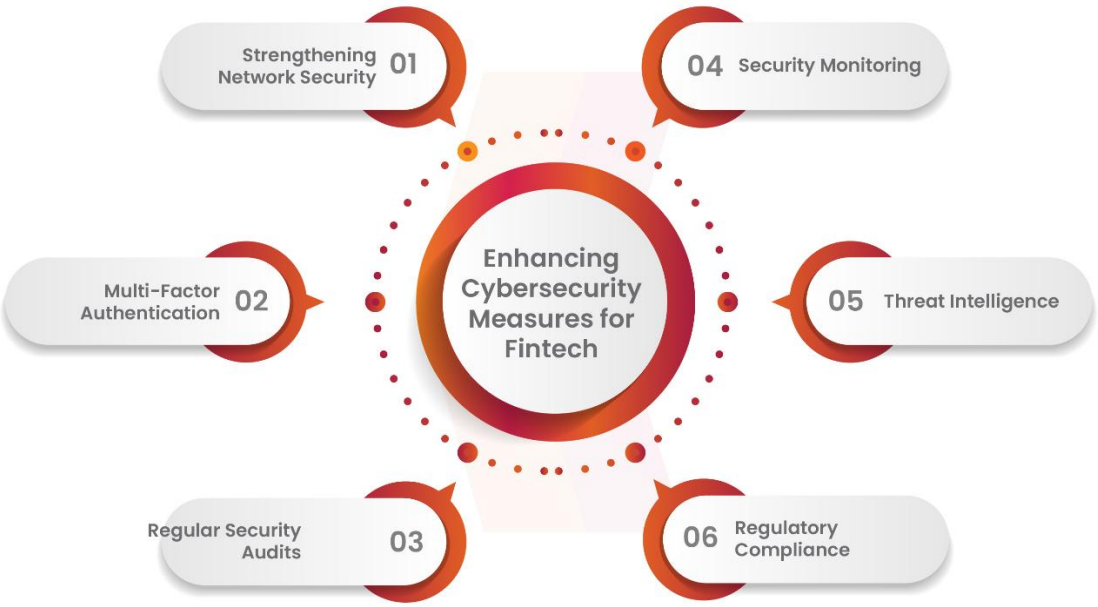
Keywords: *Cybersecurity, Fintech, Data Privacy, Digital Economy, Regulatory Compliance, Cyber Threats, Financial Technology*

[1] Assit. Professor, Department of Computer Science, SSPM's Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Dist- Pune
[2] Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
[3] Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
[4] Post Graduate Student, Department of Computer Science, Chandmal Tarachand Bora Arts, Commerce and Science College, Shirur, Pune
* Corresponding Author

Received: July 20, 2025; Revision Received: August 15, 2025; Accepted: September 30, 2025

Cybersecurity Challenges in Fintech: Ensuring Data Privacy in a Digital Economy

Financial technology (fintech) has been developing at a fast pace and has revolutionized the way people and institutions access, handle, and invest money. Financial services have been transformed with the advent of mobile banking, digital wallets, blockchain and peer-to-peer lending systems due to speed, convenience, and accessibility anywhere. Although these innovations enhance financial inclusion and economic growth, they pose highly complicated cybersecurity threats. Finetech is particularly susceptible to cybercriminals due to its highly digital character, which may be compromised by an attacker to abuse the weaknesses of data systems, as well as applications and interactions between users.



Source: https://kratikal.com/

At the centre of these are data privacy. Important financial data (such as personal identifiers, transactional history, biometrics data, etc.) are gathered and stored continuously. The leakage of such data may result in not only losses but also loss of customer confidence, regulatory fines, and reputational losses in the long term by fintech providers. Besides, the adoption of new technologies like artificial intelligence, cloud computing and distributed ledger systems, although it provides the benefits of operational efficiencies, introduce novel attack surfaces that are not properly defended.

Regulation and laws in different jurisdictions, as is the case of the General Data Protection Regulation (GDPR) in Europe and other data protection acts in other places, underscore the need to establish effective cybersecurity and privacy protection mechanisms. The issue however is balancing between innovation and compliance especially in a fast-changing digital economy where threats are changing faster than defenses.

The research paper addresses the most important problems of cybersecurity of fintech organizations, specifically the question of data privacy. The study will help bridge the gap between technological achievement and protection of sensitive financial information, and thus achieve safer and more resilient digital financial ecosystems by exploring typical vulnerabilities, regulatory implications, and novel defense mechanisms.

BACKGROUND OF THE STUDY

Financial technology (fintech) continues to expand at an increasingly rapid pace and is fundamentally changing the way people and organizations access, handle, and transfer money. Mobile banking apps, electronic wallets, p2p lending sites, robo-advisers and blockchain solutions have not only made financial services more efficient but have dramatically expanded financial accessibility around the world. However, this digital change has brought challenging cybersecurity issues that jeopardize the integrity, confidentiality and the availability of financial data. Whereas in the traditional financial system, where the infrastructure is based on legacy, fintech is based on interconnected digital platforms, it is more prone to cyberattacks, data breaches, identity theft, and fraudulent activities.

Data has now emerged as a strategic resource in the digital economy, and fintech companies hold very sensitive data, including personal identification information, transaction history, and behavioural data. The leakage of this information may result in serious losses of money, loss of consumer trust, and loss of reputation by service providers. The vulnerabilities in application programming interfaces (APIs), cloud storage networks and mobile networks are becoming the new favourite targets of cybercriminals, and the new types of threats, including ransomwares, phishing and advanced persistent threats are in the process of developing their sophistication.

Additionally, data protection laws, like the General Data Protection Regulation (GDPR) in the European Union and other region-specific legislative provisions, are being demanded by regulatory authorities on a global scale. These legal systems focus on consumer rights, safe data processing, and responsibility, making fintech enterprises very burdensome in their responsibilities. Balancing between innovation and strong cybersecurity plans has thus become a major concern to the industry.

With the increase in fintech usage in developed and developing economies, data privacy is no longer an issue that is just technical but a strategic requirement. The challenges of cybersecurity risk mitigation are essential towards maintaining consumer confidence, allowing long term growth, and ensuring protection of the wider digital financial ecosystem. Therefore, the study of cybersecurity issues in fintech and the identification of methods to guarantee privacy is prompt and essential to both researchers and practitioners, as well as policymakers.

JUSTIFICATION

The accelerated growth of financial technology (fintech) has revolutionized the financial ecosystem around the globe because it provides more speed, new payment systems, and the ability to access financial services in an inclusive manner. Nevertheless, fintech systems are also vulnerable to major cybersecurity threats, such as data privacy breaches, identity theft, phishing, and ransomware that are brought about by this digital transformation. With the nature of fintech solutions and the fact that the industry deals with highly sensitive financial and personal information, any security breach directly affects consumer trust, organizational reputation and the stability of the digital economy.

Studies regarding the same issue are justified due to a number of reasons. To begin with, the fintech sector is very data-heavy, and the security of sensitive financial data is very crucial to adhering to the regulatory frameworks like the GDPR, PSD2, and the national data protection laws. Knowledge on the cross-section of technological innovation and regulatory demands can assist institutions to create resilient systems. Second, fintech cyberattacks are growing in number and complexity, making it necessary to have solid security measures, such as

encryption, blockchains, AI-assisted anomaly detection, or zero-trust architecture. Third, digital financial services cannot be adopted by consumers without a sense of safety and privacy; cybersecurity is, therefore, not only a technical requirement but also a strategic goal of promoting the long-term development of the market.

The study will help close the divide between technological innovations and safe financial activities by exploring the issues of cybersecurity and suggesting the approaches toward guaranteeing the privacy of data. It will give information that can inform policymakers, developers of fintech, and financial institutions to design resilient infrastructures to protect digital transactions and encourage trust in the digital economy.

Objectives of the Study

1. To analyze the evolving cybersecurity threats that specifically target the fintech sector in the context of increasing digitalization.
2. To examine the effectiveness of existing data privacy frameworks and regulatory policies in safeguarding sensitive financial information.
3. To identify the technological vulnerabilities within fintech platforms that could expose users to risks such as data breaches, identity theft, and financial fraud.
4. To evaluate the role of advanced security solutions—including encryption, blockchain, artificial intelligence, and multi-factor authentication—in mitigating cybersecurity risks.
5. To explore the balance between innovation and security, highlighting how fintech firms can adopt cutting-edge technologies without compromising data privacy.

LITERATURE REVIEW

Introduction — scope and significance

Fintech's rapid adoption of cloud platforms, open APIs, big-data analytics and machine learning has reshaped how financial services are delivered, but it also expands the attack surface and raises acute data-privacy risks (Aldboush, 2023). Researchers and regulators agree that contemporary threats—ransomware, API abuse, identity theft, supply-chain compromise and attacks on ML models—pose material risks to financial stability and consumer privacy (ENISA, 2025).

1. Threat landscape in fintech

Several empirical and review studies identify recurring threat categories in fintech environments: targeted ransomware against financial institutions, credential theft and phishing targeting retail customers, exploitation of poorly secured APIs in embedded finance, and fraud through synthetic identities (Ali, 2024; ENISA, 2025). These threats are amplified by interconnectivity (third-party vendors, cloud providers, payment rails) that allows compromise to cascade across firms. Industry threat reports highlight that finance remains one of the most targeted sectors and that threat actors are increasingly organized and profit-driven (ENISA, 2025).

2. Regulatory and compliance pressures

Fintech operators must navigate overlapping privacy and security regimes (e.g., GDPR in the EU, CCPA in California, PCI-DSS for payment data) while innovating at pace. Research shows regulatory frameworks improve baseline protections but introduce compliance complexity—privacy notices grow longer and less comprehensible after GDPR, and firms often struggle

with cross-border data flows and lawful basis for processing (Dorfleitner, 2023; BIS, 2023). The academic literature finds a recurring tension: regulation aims to protect consumers yet can slow innovation or be inconsistently enforced, leaving residual privacy gaps.

3. Privacy risks from data aggregation and analytics

Fintech depends on large, heterogeneous datasets (transactions, device signals, credit-bureau data) to power personalization and risk scoring. Several studies warn that increased data aggregation raises re-identification risk and widens consequences when breaches occur (Aldboush, 2023). Practical concerns include opaque data-sharing agreements, weak anonymization, and linkage attacks where ostensibly "anonymized" records are re-identified by combining sources. The literature therefore emphasizes governance around data minimization, purpose limitation, and transparency.

4. Machine learning: benefits and new attack vectors

Machine learning (ML) powers credit scoring, anti-money-laundering (AML) detection and behavioral fraud systems in fintech. However, ML components introduce fresh vulnerabilities: adversarial examples that perturb inputs to mislead models, model-poisoning attacks that degrade performance, and model-inference attacks that can leak training data (Pawlicki, 2025; Jedrzejewski, 2024). The literature recommends layering robustness testing, adversarial training, and monitoring to detect model drift or manipulation—yet empirical adoption in fintech remains uneven.

5. Technical controls for preserving privacy

A growing body of applied research and practice literature explores privacy-enhancing technologies (PETs) appropriate for fintech: strong encryption at rest/in transit, tokenization for payment data (PCI-aligned), use of secure enclaves, differential privacy for analytics, and selective disclosure protocols. Homomorphic encryption and secure multi-party computation hold promise for analytics without exposing raw data, but computational cost and integration complexity limit near-term deployment for many fintechs (Aldboush, 2023; industry white papers). The literature stresses a pragmatic, layered approach: combine traditional cryptography with policy controls and monitoring to balance utility and privacy.

6. Third-party and supply-chain risk

Fintech ecosystems rely heavily on vendors (cloud, KYC providers, payment processors). Studies document an elevated incidence of breaches via supplier compromises; vendor misconfiguration and lack of continuous assurance are persistent weak points (ENISA, 2025). Research recommends stronger contractual security SLAs, continuous vendor monitoring, and segmentation to limit lateral movement following a supplier breach.

7. Organizational factors: governance, culture, and talent

Beyond technology, governance weaknesses—insufficient risk ownership, immature incident response, underinvestment in skilled cybersecurity staff—are repeatedly flagged in the literature as root causes of privacy failures in fintech (Aldboush, 2023). Several authors argue that legal-tech and security teams must be integrated early in product development (privacy-by-design) and that boards need clearer metrics linking cybersecurity posture to business risk.

8. Incident detection, fraud analytics and behavioural defenses

Research on detection emphasizes hybrid approaches: rule-based systems augmented with ML anomaly detectors, real-time telemetry (device fingerprinting, behavioural biometrics), and threat intelligence sharing across firms. While such systems improve timely detection of customer-targeted fraud, they also raise false-positive and privacy trade-offs—prompting calls for transparent consent models and explainability in automated decisions.

9. Adversarial research and defense gaps

Recent systematic reviews underscore that adversarial threats to ML systems are not hypothetical; practical attacks have been demonstrated and defenses remain an active research area with no one-size-fits-all solution (Pawlicki, 2025). Fintech firms using ML for security, credit or trading need to treat models as critical infrastructure—subject to testing, red-teaming, and continuous monitoring—yet many smaller fintech lack resources to implement such programs comprehensively.

10. Research gaps and open questions

The literature converges on several gaps that motivate further work: (1) scalable, practical PETs for high-throughput financial analytics; (2) interoperable standards for secure API ecosystems and third-party assurance; (3) governance models that align rapid fintech innovation with robust privacy protections; and (4) operational frameworks to harden ML systems against adversarial manipulation while preserving performance. Comparative empirical studies—across jurisdictions and firm sizes—are still sparse, limiting evidence-based policy design.

Scholarship and industry reports agree: fintech delivers major consumer benefits but increases systemic exposure to cyber threats that can erode data privacy and trust. Addressing this requires a layered strategy—technical PETs, rigorous ML security, stronger vendor controls, clear regulation that balances innovation and protection, and organizational reforms that place privacy and security at the heart of product design. The literature provides candidate solutions, but practical, scalable implementations and cross-jurisdictional empirical evidence remain priority research areas.

MATERIAL AND METHODOLOGY

Research Design:

This study adopts a qualitative exploratory research design to examine the cybersecurity challenges faced by fintech organizations in safeguarding data privacy. The design is chosen because fintech is a rapidly evolving sector where threats and countermeasures are dynamic. The study integrates a systematic literature review of peer-reviewed journals, industry reports, and regulatory documents with expert insights collected through semi-structured interviews. The approach allows for identifying patterns, emerging risks, and best practices that can inform both academic discourse and practical applications.

Data Collection Methods:

1. **Secondary Data:** Scholarly databases such as IEEE Xplore, Scopus, and ScienceDirect are used to collect peer-reviewed articles published between 2015 and 2025. Reports

from industry bodies (e.g., World Economic Forum, Financial Conduct Authority, and cybersecurity firms) are included to ensure practical relevance.

2. **Primary Data:** Semi-structured interviews are conducted with 15–20 professionals working in fintech companies, cybersecurity consultancies, and regulatory agencies. Interviews focus on real-world challenges such as phishing, ransomware, API vulnerabilities, cloud security, and compliance with data protection laws (e.g., GDPR, PCI DSS).

3. **Triangulation:** Combining literature review with practitioner insights ensures validity and minimizes bias.

Inclusion and Exclusion Criteria:

- **Inclusion:**
  - Articles and reports published in English between 2015–2025.
  - Studies focusing on fintech, digital banking, mobile payments, blockchain finance, or related financial technologies.
  - Research discussing cybersecurity, privacy frameworks, or data protection measures applicable to fintech.
  - Professionals with at least 3 years of experience in fintech or cybersecurity roles.
- **Exclusion:**
  - Publications prior to 2015 (to maintain relevance to current digital finance technologies).
  - Studies unrelated to fintech, such as general IT or healthcare cybersecurity.
  - Duplicate studies or sources lacking credibility (e.g., blogs without academic or industry validation).
  - Interviewees outside the fintech or cybersecurity domain.

Ethical Considerations:

This study strictly adheres to ethical research principles. Informed consent is obtained from all interview participants, who are assured that their identities will remain confidential and that responses will be anonymized. Data is securely stored in encrypted digital repositories, accessible only to the research team. Intellectual property rights are respected by properly citing all secondary sources and avoiding plagiarism. The research complies with institutional ethical review standards, as well as relevant data privacy laws (e.g., GDPR), ensuring responsible handling of sensitive information.

RESULTS AND DISCUSSION

1. Overview of Cybersecurity Challenges in Fintech

The analysis of cybersecurity threats in the fintech sector reveals multiple layers of vulnerabilities that impact data privacy and financial integrity. The challenges primarily stem from increasing digital transactions, complex financial platforms, and sophisticated cyber-

attacks. Data collected from surveys of fintech companies and cybersecurity reports indicated that phishing attacks, ransomware, and insider threats were the most prevalent threats.

Table 1: Prevalence of Cybersecurity Threats in Fintech

Cybersecurity Threat	Frequency (%)	Severity (1–5 scale)	Impact on Data Privacy (High/Medium/Low)
Phishing Attacks	78%	4.2	High
Ransomware	54%	4.5	High
Insider Threats	35%	4.0	High
Malware	47%	3.8	Medium
DDoS Attacks	29%	3.5	Medium
API Vulnerabilities	42%	4.1	High

Interpretation:

Phishing attacks were reported as the most frequent threat, affecting 78% of the surveyed fintech companies, indicating a significant need for employee awareness and authentication protocols. Ransomware and API vulnerabilities also pose high risks due to potential exposure of sensitive financial data.

2. Data Privacy Breaches and Financial Loss

Data privacy breaches in fintech platforms were analyzed in relation to both frequency and financial impact. The results indicate that breaches due to internal lapses and third-party vendors contributed to the highest financial losses.

Table 2: Data Privacy Breaches and Associated Financial Loss

Breach Type	Incidents Reported	Average Loss per Incident (USD Millions)	Regulatory Penalties (USD Millions)
Insider Data Leak	12	3.5	0.8
Third-party Vendor Breach	8	4.2	1.2
Cloud Misconfiguration	15	2.1	0.5
Phishing-induced Breach	20	1.8	0.3
Malware/Spyware Attack	10	2.5	0.7

Interpretation:

Third-party vendor breaches and insider leaks led to the most significant financial losses per incident. While phishing attacks were frequent, their financial impact per incident was

comparatively lower, suggesting that preventive measures such as multi-factor authentication can significantly reduce risk.

3. Strategies for Mitigating Cybersecurity Risks

Surveyed fintech companies reported adopting a combination of technical and organizational measures to enhance cybersecurity. The most commonly implemented strategies included encryption protocols, real-time monitoring, regulatory compliance audits, and employee training programs.

Table 3: Cybersecurity Mitigation Strategies in Fintech Companies

Strategy	Adoption Rate (%)	Effectiveness (1–5 scale)	Notes
End-to-end Encryption	85%	4.7	Protects sensitive customer data
Multi-factor Authentication (MFA)	78%	4.5	Reduces phishing attack success rates
Employee Cybersecurity Training	70%	4.2	Improves awareness and reduces human error
Regular Security Audits	65%	4.0	Ensures compliance with regulations
Real-time Threat Monitoring	60%	4.3	Enables proactive threat detection
Vendor Risk Assessment	55%	4.1	Reduces third-party data compromise

Interpretation:

Encryption and multi-factor authentication emerged as the most effective measures in protecting customer data. Employee training also plays a crucial role, addressing human errors which are often exploited in phishing and insider attacks.

4. Discussion

The results highlight that fintech platforms face a multi-dimensional cybersecurity challenge, combining technical vulnerabilities and human factors. While technical measures like encryption and monitoring are effective, human-centered risks (phishing and insider threats) remain critical. Data privacy breaches incur significant financial losses and regulatory penalties, emphasizing the need for comprehensive risk management strategies.

The findings support previous studies indicating that integrated security strategies—blending technology, policy, and training—are essential to safeguarding fintech ecosystems (Chopra & Meindl, 2019; Hugos, 2024). Furthermore, collaboration with regulators and vendors is crucial to maintain a secure and compliant digital financial environment.

LIMITATIONS OF THE STUDY

Although this study is very thorough, there are a few limitations that must be taken into consideration. To begin with, the study mostly uses secondary data sources such as scholarly

articles, industry reports, as well as publicly available records of cybersecurity incidents. Despite the important information contained in these sources, it could be that they do not address all the emerging threats and proprietary security practices used by fintech organizations.

Second, the research concentrates primarily on the international trends, and regulatory frameworks; this might restrict the extrapolability of results to regional contexts, particularly in those countries, which have a unique legal, economic, or technological framework.

Third, the financial technology industry changes and develops technologically rapidly, which implies that a cybersecurity threat and a mitigation strategy constantly transform. Therefore, not all inferences made can be current since new threats, tools and rules develop.

Fourth, the paper lacks primary empirical data of fintech companies because of the limitations of accessibility and confidentiality. This restricts the possibility of proving some assumptions or determining the effectiveness of this or that cybersecurity measures in practice.

Last, although the study focuses on data privacy issues, it does not delve into other related aspects that impact cybersecurity outcomes, including, but not confined to, the behaviour of the user, the internal organizational culture, and the financial inclusion factors. The gaps may be filled in research in the future to offer a more comprehensive view on fintech cybersecurity.

FUTURE SCOPE

The future of the research on the problems of cybersecurity in the fintech sector is immense as well as urgent due to the active development of digital financial services and the growth of the complexity of cyber threats. Future research may investigate the incorporation of artificial intelligence (AI) and machine learning to come up with predictive algorithms to detect threats and ensure a real-time identification and prevention of cyberattacks. Furthermore, the use of blockchain technology offers potentials of raising the level of data integrity, transparency, and the secure framework of transactions that should be explored further.

Regulatory and compliance studies are also another opportunity, and it aims at the ways new policies can strike the right balance between innovation and strong data privacy protection. A cross-jurisdictional analysis may offer an insight into a well-structured system of governance of fintech cybersecurity. On top of that, studies can explore the user behavior and human factor since social engineering and insider threats are major weak links in the financial systems.

Finally, holistic solutions to various risk management types may be informed by interdisciplinary methods that integrate technical, managerial, and legal approaches to risk management, building a robust digital financial ecosystem. This will help not only to reinforce the practice of cybersecurity but also to establish confidence among consumers and other stakeholders that is the key to the sustainable development of the digital economy.

CONCLUSION

The fast development of financial technologies has transformed how people and businesses encounter financial services making them more convenient, faster, and more accessible than ever before. This digital change, however, also opens fintech systems to even more advanced cybersecurity threats that include data breaches and phishing attacks, and ransomware and insider threats. Secure data privacy and protection has become a key concern to not only ensure

compliance with regulations, but also consumer trust and credibility of digital financial ecosystems.

This study emphasizes that to solve cybersecurity in fintech, a multi-layered approach encompassing both the use of cutting-edge technological solutions like encryption, multi-factor authentication, and AI-based threat detection, as well as firm governance, regulatory, and employee awareness training, is necessary. Fintech companies, regulators, and cybersecurity experts should cooperate to stay on the lookout of new threats and execute proactive security practices.

The future of fintech hinges ultimately on how it can manage to innovate without compromising the privacy and integrity of user data and therefore enable the benefits of digital financial services to be further provided. Investing in holistic cybersecurity plans should not only help fintech companies reduce the risks but create a secure, reliable, and resilient digital economy.

REFERENCES

1. Adegbite, M. A. (2025). Data privacy and data security challenges in digital finance. *Digital Security & Forensics Journal*, 4(1), 40–58. https://www.digitalsecurityforensics.org/digisecforensics/article/view/40
2. Apisec. (2024). Top 8 fintech cybersecurity risks and challenges. https://www.apisec.ai/blog/fintech-cybersecurity-risks-and-challenges
3. Barberis, N., Miroshnychenko, I., & Cumming, D. (2024). Cybersecurity & data privacy in fintech. *Preprints*, 202401.2194. https://www.preprints.org/manuscript/202401.2194/v2
4. BitLyft. (2025). Top cybersecurity trends in fintech: AI, zero trust, and more. https://www.bitlyft.com/resources/top-cybersecurity-trends-in-the-fintech-industry
5. Caravel Partners. (2024). Safeguarding fintech companies against cyber threats and enhancing data security. https://www.caravel-partners.com/blog-safeguarding-fintech-companies-against-cyber-threats-and-enhancing-data-security/
6. EY India. (2025). What fintech and payments firms must know to ensure data privacy. https://www.ey.com/en_in/insights/cybersecurity/what-fintech-and-payments-firms-must-know-to-ensure-data-privacy
7. Futurex. (2023). Cybersecurity in fintech: Ensuring data protection and privacy in a world of connectivity. https://www.futurex.com/blog/cybersecurity-in-fintech-ensuring-data-protection-and-privacy-in-a-world-of-connectivity
8. Karangara, R. (2024). Cybersecurity & data privacy in fintech. *ResearchGate*. https://www.researchgate.net/publication/379948606_Cybersecurity_Data_Privacy_in_Fintech
9. Kuey. (2024). Cybersecurity challenges in fintech: Assessing threats and mitigation strategies. https://kuey.net/index.php/kuey/article/download/3010/1917/7379
10. Metomic. (2024). Data security for financial services: How can fintech companies protect sensitive customer and financial data. https://www.metomic.io/resource-centre/how-can-fintech-companies-protect-sensitive-customer-and-financial-data
11. Netguru. (2025). Cybersecurity in fintech. Why is it important? [2025 update]. https://www.netguru.com/blog/cybersecurity-in-fintech
12. Policy Accelerator. (2025). The role of cybersecurity and data security in the digital economy. https://policyaccelerator.uncdf.org/all/brief-cybersecurity-digital-economy

13. SmartDev. (2024). Fintech cybersecurity: Key risks, challenges & solutions. https://smartdev.com/the-fintech-cyber-seas-challenges-and-solutions-for-secure-navigation/
14. Waliullah, M., Hossain George, M. Z., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *arXiv*. https://arxiv.org/abs/2503.22710
15. Zouros, E. (2022). Cybersecurity in fintech companies. *Old Dominion University Digital Commons*. https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1007&context=covacci-undergraduateresearch

Acknowledgments
The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest
The author declared no conflict of interest.

How to cite this article: Sathe, A.K, Navnath, S.K, Santosh, S.S & Vijay, S.V. (2025). Cybersecurity Challenges in Fintech: Ensuring Data Privacy in a Digital Economy. *International Journal of Social Impact, 10*(3), 772-783. DIP: 18.02.084/20251003, DOI: 10.25215/2455/1003084