**Educational Administration: Theory and Practice**
2024, 30(4), 9262-9265
ISSN:2148-2403
https://kuey.net/

**Research Article**

# Cyber Security And Its Importance With Special Reference To Fintech Companies In Chennai

Meena Akileswaran[1*], Dr. S. Vennilaa Shree[2]

[1*]Research Scholar, VISTAS, Pallavaram, Chennai
[2]Professor, Department of Commerce, Vel's University, Pallavaram, Chennai

**Citation:** Meena Akileswaran, et al (2024), Cyber Security And Its Importance With Special Reference To Fintech Companies In Chennai, *Educational Administration: Theory and Practice*, *30*(4), 9262-9265, Doi: 10.53555/kuey.v30i4.3476

**ARTICLE INFO**

**ABSTRACT**

Cybersecurity in fintech is a multifaceted discipline that focuses on safeguarding financial services and transactions in the digital realm. As fintech continues to evolve, so do the associated security challenges, making it an ongoing and dynamic area of concern for both financial institutions and consumers.

## I. INTRODUCTION

Cybersecurity in fintech is crucial because the financial industry relies heavily on technology and the internet to provide services. The success of fintech companies is heavily dependent on cybersecurity. It goes beyond mere protection of networks or systems from malicious threats; it encompasses the guarantee of secure financial transactions, the protection of sensitive data, and the establishment of trust with customers. Here are some key points to understand about cybersecurity in fintech:

**Data Protection:** Fintech companies deal with sensitive financial data, including personal information and financial transactions. Protecting this data from unauthorized access and breaches is a top priority. Measures like encryption, access controls, and data anonymization are commonly employed.

**Authentication and Authorization:** Strong user authentication and authorization mechanisms are essential. This includes multi-factor authentication (MFA) and robust identity verification processes to ensure that only authorized individuals can access financial services.

**Secure Communication:** Secure data transmission over the internet is critical. This involves the use of encryption protocols (e.g., SSL/TLS) to safeguard data as it travels between the user's device and the fintech platform's servers.

**Vulnerability Assessment and Patch Management:** Regularly scanning for vulnerabilities in software and promptly applying patches and updates is essential to prevent known security weaknesses from being exploited.

**Fraud Detection:** Fintech companies employ various fraud detection systems, such as machine learning and artificial intelligence algorithms, to identify unusual or suspicious patterns in transactions and account activity.

**Regulatory Compliance:** Fintech companies must adhere to various financial regulations and data protection laws. Compliance with these regulations is a fundamental aspect of cybersecurity in fintech.

**Incident Response:** Fintech companies should have well-defined incident response plans in place to react quickly and effectively in the event of a security breach or cyberattack. This includes notifying affected parties and regulatory authorities as required.

**User Education:** Educating users about best practices in online security, such as choosing strong passwords and recognizing phishing attempts, is important in preventing security breaches.

**Third-Party Risk Management:** Fintech companies often rely on third-party services and vendors. Assessing and managing the security risks associated with these partnerships is crucial.

**Blockchain and Cryptocurrencies:** Fintech innovations like blockchain technology and cryptocurrencies bring their own security challenges, such as wallet security, smart contract vulnerabilities, and protection against crypto theft.

**Regulatory Sandboxes:** Some countries have introduced regulatory sandboxes where fintech companies can test their innovations in a controlled environment with regulatory oversight. This can help strike a balance between innovation and security.

**AI and Machine Learning:** Fintech companies are increasingly using AI and machine learning to enhance security. These technologies can help in threat detection, fraud prevention, and risk assessment.

Data breaches impose a significant burden on fintech firms, and the costs extend far beyond mere financial considerations. Such incidents can result in substantial recovery expenses, legal fines due to compliance breaches, customer attrition driven by damaged trust, enduring harm to brand reputation, and the risk of losing market share to competitors with more robust cybersecurity practices. Cyberattacks in the fintech industry can have far-reaching consequences beyond financial losses, including breaches of compliance standards and erosion of customer trust.

- Fintech companies have a dual responsibility to protect both customer data and financial assets. This dual responsibility is especially critical because fintech firms often act as custodians of sensitive financial information and assets.
- Prime Target for Attackers: Fintech companies are prime targets for cybercriminals due to the potential for significant financial gain. The digital nature of fintech operations and the sheer volume of financial transactions and data make them attractive targets.
- Proactive Cybersecurity: The emphasis on proactive cybersecurity is essential. Waiting for a breach to occur and then reacting is not sufficient. Fintech companies must take preemptive measures to identify and mitigate vulnerabilities before they can be exploited.
- Penetration Testing (Pentesting): Penetration testing is an important proactive cybersecurity measure. It involves simulating cyberattacks to assess the security of a system, network, or application. By identifying vulnerabilities and weaknesses, companies can take steps to remediate them before malicious actors can exploit them.
- Risk Management: Robust risk management policies are vital. Fintech companies need to identify potential risks, assess their impact, and put mitigation measures in place. This can include everything from security training for employees to comprehensive incident response plans.

The mention of specific types of cyberattacks, such as phishing, malware, and ransomware, highlights the diversity of threats fintech companies face. Each type of attack requires its own set of preventive and protective measures.

A 2019 report revealed that almost 100% of fintech companies had issues related to privacy, security, and compliance, owing to APIs, subdomains, and abandoned web applications. In 2023, these threats are much more sophisticated and dangerous for a company.

In conclusion, the fintech industry is highly attractive to cybercriminals, making robust cybersecurity measures a necessity. Fintech companies must adopt a proactive stance in protecting their customers' data and financial assets, as well as complying with relevant regulations. Cybersecurity measures, like penetration testing and comprehensive risk management, are critical components of a well-rounded cybersecurity strategy in the fintech sector.

## II. REVIEW OF LITERATURE

Gurdip Kaur (2021) in the book, Understanding Cybersecurity Management in FinTech, uncovers the idea of understanding cybersecurity management in FinTech. It emphasizes on the importance of cybersecurity for financial institutions by illustrating recent cyber breaches, attacks, and financial losses. The book delves into understanding cyber threats and adversaries who can exploit those threats. It advances with cybersecurity threat, vulnerability, and risk management in FinTech. The book helps readers understand cyber threat landscape comprising different threat categories that can exploit different types of vulnerabilities identified in FinTech. It puts forward prominent threat modelling strategies by focusing on attackers, assets, and software and addresses the challenges in managing cyber risks in FinTech. The authors discuss detailed cybersecurity policies and strategies that can be used to secure financial institutions and provide recommendations to secure financial institutions from cyber-attacks.

Ademola Adeyoju (2021) in Cybercrime and Cybersecurity: FinTech's Greatest Challenges: This highlights causes for the rise of FinTech companies and activated the FinTech transformation that the world is currently witnessing.

From payments and remittances to lending and wealth management, FinTech continues to change the way we live and bank. But by virtue of their operations, FinTech companies constitute a particularly attractive target for cybercriminals. This article examines how cybercrime affects FinTech companies—mostly startups—and how these companies protect their data and infrastructure.

Cybercrime and Cyber Security in Fintech by JARC Jayalath highlights that Fintech companies have disrupted the financial industry by means of the way customers are served with their financial needs. This has happened with the usage of immerging technologies such as Artificial Intelligence, Robotic Process Automation, Natural Language Processing, Facial Recognition, Data Analytics etc. and the development of the supporting digital technology infrastructure by using the benefit of the enhanced digital literacy of new generation customers by providing a great deal of customer convenience by delivering easily accessible and fast service to customers. As a result of the digital disruption that happened due to this Fintech initiative and the demand of especially the new generation customers, established financial companies such as banks also

followed with Fintech initiatives either with the collaboration of startup Fintech companies or by developing the Fintech initiative internally. Digital financial platforms have thereby become highly critical hence Fintech companies had to look at implementing reliable digital infrastructure and when financial platforms were more opened to the public internet, more and more cyber threats to the systems also increased rapidly. Therefore, it had become a high necessity for the Fintech companies and the Banks and Finance companies who provides digital solutions to build a structured Digital Technology Infrastructure considering resilience, performance and security to thrive in the highly competitive Digital Financial landscape

Fintech Issues and Challenges in India by Dr. S. P. Sreekala talks about new finance technologies (FinTech) that have erupted around the arena. This paper offers coherent studies on subject matters formulated via attention organization meetings with policymakers and teachers and is also based totally on a crucial evaluation of the literature. They have outlined seven key research gaps with questions that might shape the idea of an educational look. If these are addressed it would assist this location to grow to be a long-time educational area.

Fintech firms and banks sustainability: Why cybersecurity risk matters? By Khakan Najaf, Md Imtiaz Mostafiz, and Rabia Najaf: In the new and evolving digitalized world, the cybersecurity threats have placed the assets and information of corporations, institutions, governments, and individuals at constant risk. Banks are not an exception. Due to the high demand for a tailored portfolio of financial products, the availability of sophisticated communication and advance transaction mechanisms lead to an emergence of a new type of competitor known as financial technology service (i.e., fintech). The collaboration between these fintech organizations and banks has recently increased to provide fine-tuned service to the consumer and satisfy emerging market needs. However, this collaboration between banks and fintech firms has triggered significant cybersecurity risk. Hence, the dilemma is whether the bank should embrace such collaboration to resuscitate the profit margin or be pragmatic, and shirk to eliminate sustainability risk? They have argued that the alliance between bank and fintech firms triggers a high-level of cybersecurity risk. We propose a theoretical model and discuss various types of cybersecurity risks. The benefit (or cost-if any) of having alliance could be enormous in yielding profitability and increase sustainability if both fintech and banks collaboratively abate the cybersecurity risks.

Challenges in Fintech Security, by C H Patil: FinTech, or new financial technologies, has exploded globally. As a result, over the past five years, academic writing on fintech has significantly increased. Research often lacks a clear research aim and is just loosely connected. There are still significant research gaps and crucial questions. Before this field is considered an established academic discipline, more work needs to be done. This paper presents logical research issues regarding security that were developed through focus groups with academics and policymakers and are also based on an evaluation of the literature.

## III. OBJECTIVES OF THE STUDY

i. Determine the problems fintech companies face in financial transactions.
ii. What are the cybercrimes that are met. Examine the need to use several cyber security measures.
iii. Determine the level of cyber risk and challenges involved in fintech companies.

## IV. HYPOTHESIS

1) There is a positive correlation between the level of cybersecurity awareness and practices within fintech companies in Chennai.
2) Fintech companies in Chennai that demonstrate a high level of regulatory compliance also exhibit more robust cybersecurity measures.
3) Fintech companies adopting innovative technologies, such as blockchain and AI, face both increased cybersecurity challenges and opportunities for enhancing overall security.

## V. RESEARCH METHODOLOGY

The research approach adopted for the study is as below:
- Interviews/Surveys: Engaged with cybersecurity professionals in selected companies. Used open-ended questions to collect detailed information on specific practices.
- Document Review: Gathered and analyzed relevant documents to identify common cybersecurity measures.

## VI. DATA ANALYSIS AND RESULTS

The following research questions were assessed that guided in framing the scope of study.

a) What is the current state of cybersecurity awareness and practices among fintech companies in Chennai?

Effective cybersecurity measures are crucial for financial services to ward off potential losses. By implementing network security, intrusion detection systems, malware protection, and other cybersecurity protocols, financial institutions can thwart cyber-attacks and minimize their repercussions. While

cybersecurity threats are likely to persist in the evolving fintech landscape, maintaining vigilant awareness and continuous monitoring is paramount for success in this expanding marketplace. A strong cybersecurity foundation plays a pivotal role in enhancing the overall cybersecurity landscape in India by protecting data and thwarting financial fraud within the fintech sector.

b) How do fintech companies in Chennai perceive the importance of cybersecurity in their operations?
c) What cybersecurity measures and protocols are commonly employed by fintech companies in Chennai to protect sensitive financial data?

The most common answers to this question were firewalls and encryption.

d) To what extent do fintech companies in Chennai comply with relevant cybersecurity regulations and standards?
e) What challenges do these companies face in maintaining regulatory compliance, and how do they address these challenges?

Data security: A high-level security app can be established to increase security
Lack of Mobile and Tech Expertise: The mobile must have the features like NFC chip in shops, QR code, two-factor authentication, etc. to enable users with fintech app development services.
Big Data and AI Integration: Combining AI and big data requires instructing AI through machine learning, a process that demands substantial data for system training. Many banking apps face challenges in processing and retrieving extensive datasets. To address this issue, a viable solution involves employing a one-shot learning model. This model facilitates training the machine learning system with smaller datasets, offering an effective resolution to the limitations posed by the processing capacity of banking apps.

## VII. DISCUSSION OF RESULTS

Cybersecurity is of paramount importance, particularly in the context of fintech companies in Chennai. The fusion of financial technology with digital operations makes these entities susceptible to a range of cyber threats. Safeguarding sensitive financial data and ensuring the integrity of digital transactions are critical aspects for the smooth functioning of fintech firms.
Cybersecurity is a linchpin for the success, trustworthiness, and resilience of fintech companies in Chennai. As these entities continue to drive financial innovation, prioritizing and investing in cybersecurity measures is imperative for sustained growth and customer satisfaction.