Chapter 16
Emerging Trends and Challenges of Cyber Security in Fintech: A Conceptual Overview

S. Anitha
Department of Management, Central University of Tamil Nadu, India

S. Visalakshmi
Department of Management, Central University of Tamil Nadu, India

ABSTRACT

The Fintech-driven digital financial ecosystem has a tremendous impact on India's economic growth and development. All industries and business sectors are facing challenges as a result of digital transformation. Fintech employs technology to improve and automate financial services, whereas cybersecurity ensures the security of these services and data. This study explores the crucial role that cybersecurity plays in safeguarding sensitive information, critical infrastructure, and technological ecosystems from a multitude of threats in financial technology. It deliberates numerous cyber threats, ranging from phishing attacks to sophisticated malware, and highlights the importance of proactive measures such as encryption, access controls, and intrusion detection systems. This study reveals that Fintech innovations have a significant impact on the economy and society by providing access to the digital economy while cybersecurity is crucial in leveraging the benefits of Fintech.

1. INTRODUCTION

Fintech has become an everyday demand in today's setting of digitalization in all financial activities, and use of the services has expanded. Fintech has become an effective strategy for promoting financial inclusion (Ediagbonya et al 2023). However, as more people utilise digital platforms, cyber dangers have increased as well. These attacks can seriously affect financial stability and prevent people from reaping the benefits of financial inclusion. The promotion of financial inclusion in Fintech depends substantially on cybersecurity. Securing of data and information has paved way to build a strong cybersecurity plat-

DOI: 10.4018/979-8-3693-2346-5.ch016

form. Protecting computer systems, networks, and data from digital threats, attacks, and unauthorised access is known as cybersecurity. It involves a range of techniques, processes, and tools to ensure the confidentiality, integrity, and availability of information in digital environments. As technology advances, cybersecurity plays a crucial role in safeguarding personal, organizational, and societal interests from cybercrimes, data breaches, and other malicious activities. According to Inc42's recent report, India is one of the world's fastest-growing Fintech sectors, with a present valuation of $584 billion and a projected value of $1 trillion by 2025.While financial literacy, awareness, and regulatory stability remain big obstacles for the sector, cybersecurity is a fundamental block to its growth.

A cyberattack on a Fintech firm could result in financial losses, identity theft, and reputational harm. Fintech organisations may protect themselves from the most frequent cybersecurity risks and keep their clients' data safe by having a robust cybersecurity programme. There were 1,829 documented cyber incidents in the financial industry globally in 2022, compared to 2,527 the previous year. In general, the amount of data breaches has declined over the last two years, falling from 690 in 2021 to 477 in 2022. In reality, the majority of contemporary Financial Service Institutions (FSIs) use IT-related strategies to assist in providing financial services (Gai et al 2018). Therefore, cybersecurity is vital for Fintech companies to secure and shield their customers' data from the cyber threats. Digital financial services are in greater demand, and there are more potential for financial inclusion. The purpose of the study is to determine the components that influence cybersecurity, its challenges and analyse the current cybersecurity developments in financial technology. This study also emphasises the importance of continual research and adaptation to keep ahead of evolving cyber threats and ensure the resilience of digital environments as technology advances.

2. LITERATURE REVIEW

Cyber security is becoming increasingly important in order to safeguard oneself in the digital realm. Despite the advancement in Fintech, more cybersecurity and law enforcement capabilities are required to protect cyberspace. Privacy and trust (Liao Liu et al 2011) have received much attention in the literature for their relationships with online transactions. Najaf et al (2020) discusses the increasing collaboration between traditional banks and Fintech firms to enhance customer service and profitability. This collaboration involves cybersecurity concerns such as data breaches and vulnerabilities that must be managed carefully. Addressing these risks and preserving customer trust are critical to the long-term viability of these alliances. To accomplish this, banks and fintech companies should collaborate on cybersecurity measures, follow regulations, and seek cyber insurance. The findings of the study highlighted that decision to collaborate should strike a balance between profitability and sustainability, and it should include extensive due diligence and constant monitoring of cybersecurity practises. With the growth of Fintech 3.5, comprehensive cybersecurity measures are required to combat the rise in cybercrime (Nagasundari et al 2021). The author investigates the importance of cybersecurity, namely AI-powered solutions, in preventing and detecting financial fraud. It encompasses all aspects of cybersecurity, including tools, applications, difficulties, and regulatory concerns. The study focuses on the vital importance of cybersecurity in the complicated IoT context. Similarly, Jayalath et al (2021) examined vital characteristics that are fundamental to the digital technology infrastructure of fintech businesses and identified strategies for increasing cybersecurity. The study analyses and evaluates the fundamental elements of digital technology infrastructure, such as cloud computing, data analytics, and blockchain technology, which