Abstract

The financial sector is increasingly vulnerable to cyber threats due to its reliance on digital infrastructure and the vast amounts of sensitive financial data it processes. This study examines the key cybersecurity threats affecting financial institutions, including data breaches, phishing attacks, ransomware, insider threats, and regulatory non-compliance. It further explores the security protocols used to mitigate these risks, such as multi-factor authentication (MFA), encryption, artificial intelligence (AI)-driven fraud detection, and blockchain technology. Additionally, the study investigates data privacy concerns and regulatory challenges faced by financial institutions, assessing compliance with frameworks such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). The research also highlights fraud prevention strategies, including real-time transaction monitoring and behavioral analytics, to counter financial cybercrime. By analyzing existing literature and regulatory policies, this study provides insights into strengthening cybersecurity resilience in financial services. The findings underscore the need for a proactive, multi-layered security approach that integrates advanced technologies, regulatory compliance, and continuous risk assessments to protect financial data and maintain institutional trust.