A STUDY ON CYBER SECURITY RISKS IN ONLINE BANKING

A. Lavanya
Assistant Professor
Department of Commerce
Sir C R Reddy College, Eluru
Mail id: allalavanya04@gmail.com

K. Venkata Satya Sai Anil(3234507)
UG Scholar
Department of Commerce
Sir C R Reddy College, Eluru

M. Sree Jyothika(3234520)
UG Scholar
Department of Commerce
Sir C R Reddy College, Eluru

Ch. Neeladri(3244707)
UG Scholar
Department of Commerce
Sir C R Reddy College, Eluru

Submitted: 08-11-2025 *Accepted: 22-12-2025* *Published: 29-12-2025*

ABSTRACT

The rapid growth of online banking has fundamentally transformed the delivery of financial services by enabling customers to perform transactions, manage accounts, and access banking facilities through digital platforms. Driven by increased internet penetration, smartphone usage, and the demand for convenience, online banking has become an essential component of modern financial systems. However, this digital transformation has also intensified cyber security concerns, as financial institutions handle large volumes of sensitive customer and transaction data. Ensuring cyber security is therefore critical to maintaining trust, financial stability, and regulatory compliance within the banking sector.

This study examines the major cyber security risks associated with online banking, including phishing attacks, malware infections, identity theft, man-in-the-middle attacks, and data breaches. A descriptive and analytical research methodology is adopted, primarily based on secondary data collected from academic journals, regulatory reports, industry publications, and documented case studies. The analysis focuses on identifying common attack patterns, vulnerable system components, and the role of human factors in cyber incidents.

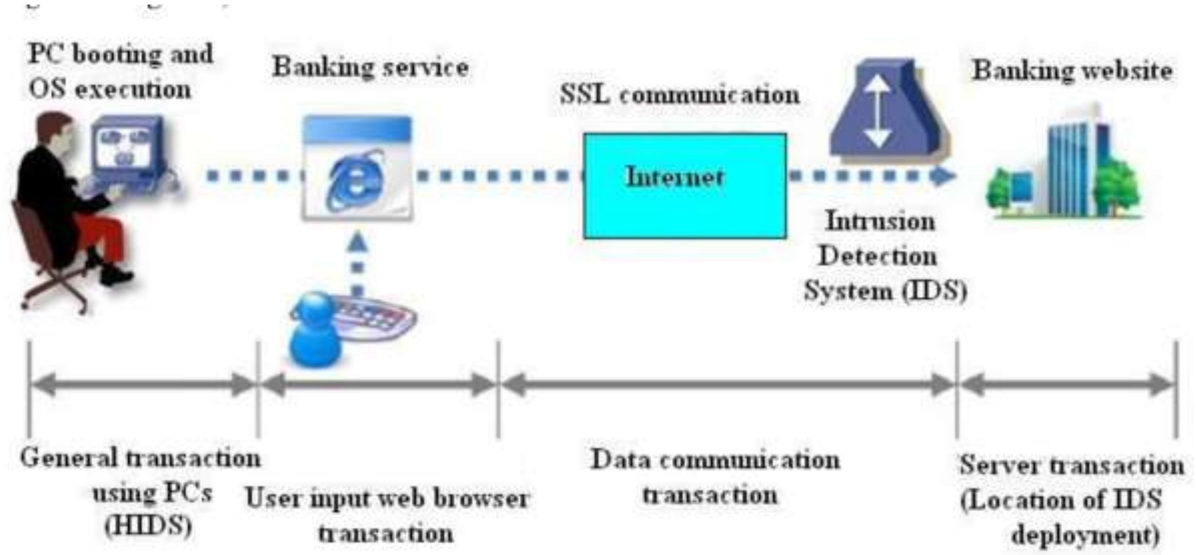
The key findings reveal that phishing and malware attacks remain the most prevalent threats, largely due to user unawareness and weak security practices. The study highlights that a multi-layered security approach combining technical safeguards, organisational policies, regulatory compliance, and user education significantly reduces cyber risk exposure. The practical significance of this research lies in providing valuable insights for banks, regulators, and customers to strengthen cyber security strategies and promote safer online banking practices.

Keywords: Cyber security, Online banking, Phishing attacks, Malware, Financial fraud, Data privacy, Risk management

INTRODUCTION

The banking sector has undergone a profound transformation over the past few decades, largely driven by advances in information and communication technologies. Traditional banking, which once relied heavily on physical branches and manual processes, has progressively evolved into a technology-driven service industry. The introduction of automated teller machines (ATMs) marked an early step in this evolution, followed by telephone banking and, eventually, fully-fledged online banking platforms. Online banking services initially offered basic functionalities such as balance enquiries and fund transfers, but have since expanded to include bill payments, loan management, investment services, and real-time customer support. This steady evolution reflects the growing emphasis on efficiency, accessibility, and customer-centric service delivery in modern banking systems (Laudon & Laudon, 2020).

Digital transformation has played a central role in reshaping the banking industry. The integration of digital technologies such as mobile applications, cloud computing, big data analytics, and application programming interfaces (APIs) has enabled banks to redesign their operational models and service offerings. Digital transformation has not only reduced operational costs but has also improved transaction speed, accuracy, and scalability. Moreover, it has enabled banks to compete with emerging financial technology (fintech) firms by offering innovative and personalised services. According to Anderson (2020), digital platforms have become the backbone of contemporary financial systems, allowing banks to process massive volumes of transactions securely and efficiently. However, this transformation has also introduced new complexities and dependencies on interconnected digital infrastructures.


PC booting and OS execution
Banking service
SSL communication
Internet
Banking website
Intrusion Detection System (IDS)
General transaction using PCs (HIDS)
User input web browser transaction
Data communication transaction
Server transaction (Location of IDS deployment)

The increasing dependence on internet-based financial transactions is another defining characteristic of modern banking. Customers now expect uninterrupted, round-the-clock access to banking services through web portals and mobile applications. The widespread availability of high-speed internet and smartphones has accelerated the adoption of digital banking, particularly in developing economies. Online payment systems, digital wallets, and instant fund transfer mechanisms have become integral to everyday financial activities. Reports indicate that a significant proportion of retail banking transactions are now conducted online, reducing reliance on physical branches (OECD, 2020). While this shift has enhanced convenience and financial inclusion, it has also increased exposure to cyber threats, as financial transactions are conducted over public and private networks that may be vulnerable to attacks.

As online banking systems become more complex and interconnected, the need for strong cyber security mechanisms has become increasingly critical. Online banking platforms store and transmit highly sensitive information, including personal identification details, authentication credentials, and transaction records. Any compromise of this data can result in severe financial losses, identity theft, and erosion of customer trust. Cybercriminals exploit technical vulnerabilities, weak security configurations, and human errors to gain unauthorised access to banking systems. Studies have shown that the financial sector is among the most frequently targeted industries for cyber attacks due to the direct monetary benefits associated with successful breaches (Verizon, 2023). Consequently, ensuring robust cyber security has become a strategic priority for banks and regulators worldwide.

Cyber security in online banking encompasses a broad range of measures aimed at protecting information assets and ensuring service continuity. These measures include encryption, authentication mechanisms, intrusion detection systems, and secure network architectures. However, technological safeguards alone are insufficient to address the evolving threat landscape. Human factors, such as poor password practices and susceptibility to social engineering attacks, continue to undermine even the most advanced security systems (Hadnagy, 2018). Phishing attacks, for instance, rely primarily on deceiving users rather than exploiting software vulnerabilities, making them particularly difficult to prevent through technical means alone. This highlights the importance of combining technological solutions with organisational policies and user education.

The motivation for this study arises from the growing gap between the rapid adoption of online banking services and the persistent challenges associated with cyber security. Despite significant investments in security technologies, cyber incidents in the banking sector continue to increase in frequency and sophistication. Regulatory bodies have introduced cyber security frameworks and guidelines to strengthen resilience, yet compliance alone does not guarantee protection against emerging threats (Basel Committee on Banking Supervision, 2021). There is therefore a pressing need for comprehensive research that examines cyber security risks from a holistic perspective, considering technological, organisational, and behavioural dimensions.

The significance of this study lies in its potential contribution to both academic research and practical applications. From an academic standpoint, the study synthesises existing literature on cyber security risks in online banking and identifies key threat vectors and mitigation strategies. Practically, the findings can assist banks in strengthening their security frameworks and help policymakers refine regulatory approaches. Additionally, the study underscores the role of customer awareness in reducing cyber risk, thereby emphasising the shared responsibility of banks and users in ensuring secure online banking environments. As digital banking continues to expand, such insights are essential for sustaining trust and stability in financial systems.

LITERATURE SURVEY

The rapid expansion of online banking services has attracted significant research attention due to the growing cyber security risks associated with digital financial transactions. Early studies on online banking security primarily focused on system reliability and basic authentication mechanisms. However, with the increasing sophistication of cyber threats, recent literature has shifted towards analysing complex attack vectors and comprehensive defence strategies. Anderson [1] highlighted that as banking systems become more interconnected, vulnerabilities multiply across networks, applications, and user interfaces, making cyber security a fundamental design requirement rather than an auxiliary feature. Several researchers have identified phishing attacks as one of the most dominant threats in online banking environments. Hong [10] provided an extensive analysis of phishing techniques, demonstrating how attackers exploit user trust through fraudulent emails and spoofed websites. Florêncio and Herley [7] further examined the economic aspects of phishing and concluded that the low cost and high success rate of such attacks make them particularly attractive to cybercriminals targeting banking customers. These findings indicate that technical safeguards alone are insufficient unless accompanied by strong user awareness initiatives.

Malware-based attacks have also been widely discussed in the literature as a major risk to online banking systems. Egele et al. [5] presented a comprehensive survey of malware analysis techniques and explained how keyloggers and banking trojans are used to capture sensitive credentials from infected devices. Symantec [18] reported that malware attacks targeting financial institutions have increased steadily, with attackers employing advanced obfuscation techniques to evade detection. Such studies emphasise the need for continuous monitoring and adaptive security mechanisms within banking infrastructures. Man-in-the-middle (MITM) attacks represent another critical area of concern in online banking security research. Conti et al. [4] analysed various MITM attack scenarios and highlighted how insecure communication channels and public networks expose banking transactions to interception and manipulation. Their work demonstrated that even encrypted systems may be vulnerable if authentication protocols are weak or improperly implemented. This reinforces the importance of end-to-end security design in online banking platforms.

Identity theft and account takeover attacks have also received considerable attention in academic research. Alasmary et al. [20] discussed how stolen personal information is exploited to gain unauthorised access to banking accounts, leading to significant financial losses. Verizon's Data Breach Investigations Report [19] consistently ranks credential theft among the leading causes of financial data breaches, further validating the findings of academic studies. These works underline the growing need for robust identity management and authentication systems. Insider threats pose a unique challenge in online banking, as they originate from individuals with legitimate access to systems. Greitzer et al. [8] analysed both malicious and unintentional insider threats and found that inadequate security training and poor access control significantly increase risk. Unlike external attacks, insider threats are difficult to detect using conventional security tools, prompting researchers to advocate for behavioural monitoring and strict privilege management within banking organisations.

The role of user awareness and behaviour in cyber security has been widely explored in recent literature. Bada et al. [3] examined the effectiveness of cyber security awareness programmes and concluded that many initiatives fail to bring lasting behavioural change among users. Hadnagy [9] further emphasised that social engineering attacks succeed primarily due to psychological manipulation rather than technical weaknesses. These studies collectively suggest that educating users is as important as deploying advanced security technologies in online banking systems. From a technological perspective, encryption and cryptographic protocols have been extensively studied as foundational security measures. Stallings [17] provided a detailed discussion on cryptographic techniques used to protect data confidentiality and integrity in online transactions. While encryption is widely adopted, researchers argue that poor key management and weak implementation can undermine its effectiveness. Consequently, secure cryptographic practices remain a central theme in online banking security research.

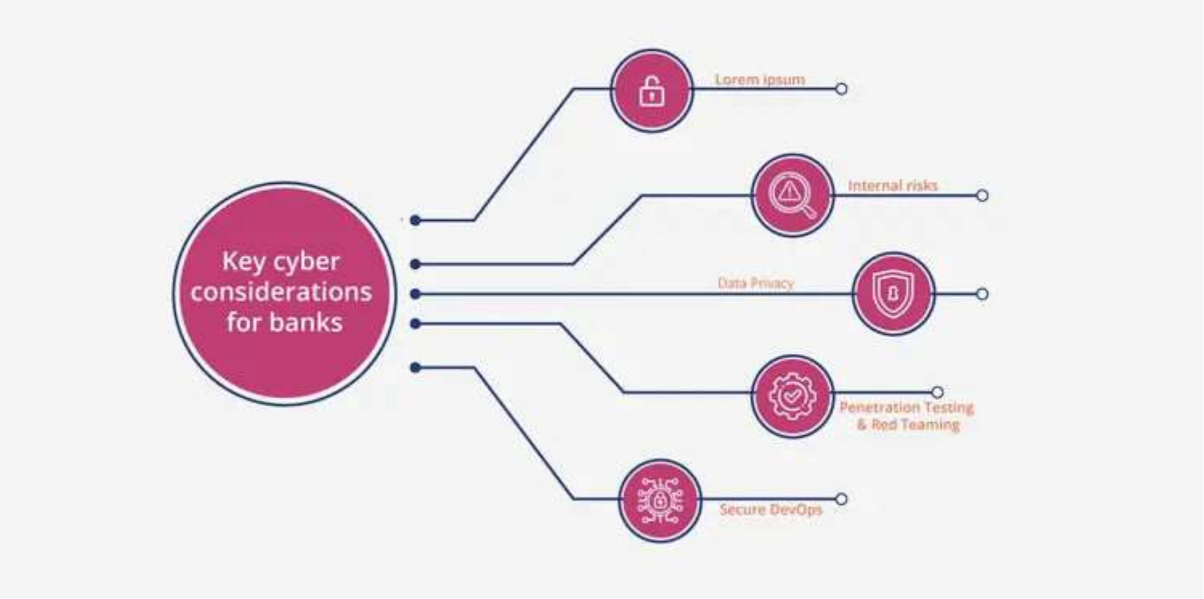
Recent studies have increasingly explored the application of artificial intelligence and machine learning in detecting cyber fraud. Sharma and Mathur [16] demonstrated that AI-based fraud detection systems can analyse transaction patterns in real time and identify anomalies more accurately than traditional rule-based systems. These findings suggest that intelligent security solutions can significantly enhance threat detection capabilities in online banking environments. Regulatory and compliance-related aspects of cyber security have also been discussed extensively in the literature. The Basel Committee on Banking Supervision [2] introduced cyber-resilience frameworks that encourage banks to adopt risk-based security approaches. Similarly, ISO/IEC 27001 [11] provides guidelines for information security management systems, which have been widely referenced in academic and industry research. OECD [14] highlighted that regulatory compliance improves baseline security but must be complemented by proactive risk management strategies to address emerging threats.

Regional studies have further enriched the literature by examining country-specific cyber security challenges. The Reserve Bank of India [15] outlined a cyber security framework tailored to Indian banking systems, focusing on governance, risk assessment, and incident response. Such studies highlight the importance of contextualising cyber security measures based on regulatory and infrastructural differences across regions. Overall, the literature indicates that cyber security risks in online banking are multifaceted, involving technological vulnerabilities, human factors, and organisational weaknesses. While significant progress has been made in developing technical solutions, researchers consistently point to the need for integrated security frameworks that combine advanced technologies, regulatory compliance, and continuous user education. This study builds upon existing research by synthesising these perspectives and emphasising a holistic approach to managing cyber security risks in online banking systems.

Cyber Security Risks in Online Banking

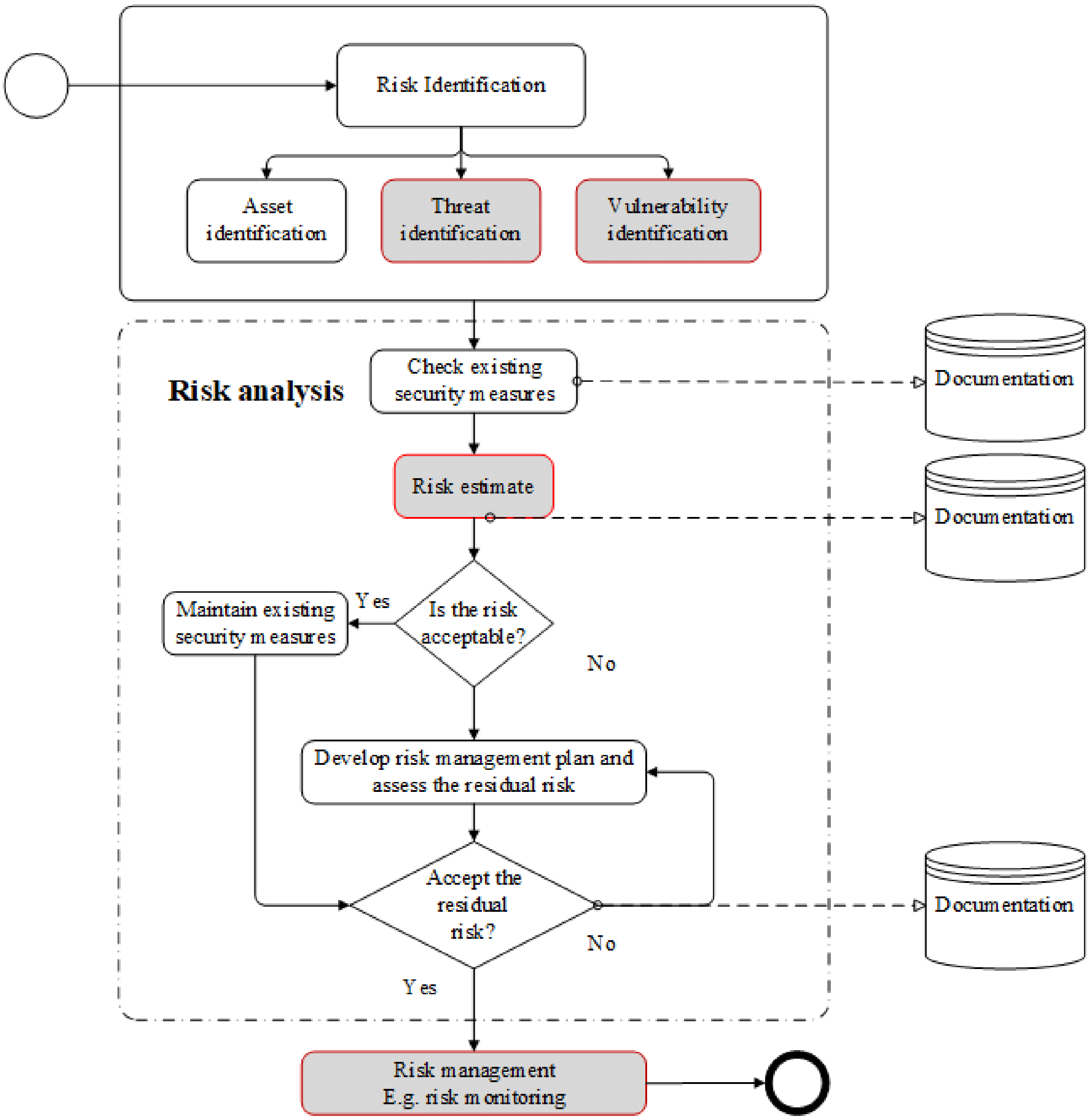
Online banking systems face a wide range of cyber security risks that can compromise data integrity and financial stability. One of the most common threats is phishing, where attackers use deceptive emails or messages to trick users into revealing sensitive information. These attacks often mimic legitimate banking communications, making them difficult to detect.

Malware attacks pose another significant risk. Malicious software such as keyloggers and trojans can be installed on users' devices, enabling attackers to capture login credentials and transaction details. Ransomware attacks can also disrupt banking operations by encrypting critical data and demanding payment for its release. Man-in-the-middle attacks occur when attackers intercept communication between users and banking servers. By exploiting insecure networks, attackers can alter or steal transaction data without the knowledge of either party. Identity theft and account takeover attacks involve unauthorised access to user accounts, often resulting in fraudulent transactions. Insider threats, arising from malicious or negligent employees, also pose serious risks to banking systems. Additionally, large-scale data breaches can expose sensitive customer information, leading to long-term financial and reputational damage.


Key cyber considerations for banks
Lorem ipsum
Internal risks
Data Privacy
Penetration Testing & Red Teaming
Secure DevOps

Research Methodology

This study adopts a descriptive and analytical research methodology to examine cyber security risks in online banking. The research is primarily based on secondary data collected from academic journals, conference proceedings, industry reports, and credible online sources. A systematic review of existing literature was conducted to identify common cyber threats, vulnerabilities, and mitigation strategies. The data were analysed to understand patterns in cyber-attacks and their impact on banking operations and customers.


Risk Identification
Asset identification
Threat identification
Vulnerability identification
Risk analysis
Check existing security measures
Documentation
Risk estimate
Documentation
Is the risk acceptable?
Yes
Maintain existing security measures
No
Develop risk management plan and assess the residual risk
Accept the residual risk?
No
Documentation
Yes
Risk management E.g. risk monitoring

The study also incorporates a conceptual analysis of recent cyber incidents in the banking sector to illustrate real-world implications of security breaches. Although the research does not involve primary data collection, the use of diverse secondary sources ensures a comprehensive understanding of the subject. The methodology has certain limitations, including reliance on published data and the absence of empirical validation through surveys or experiments. Nevertheless, the approach provides valuable insights into the current state of cyber security in online banking.

Data Analysis and Discussion

The analysis of existing studies reveals a steady increase in cyber attacks targeting online banking platforms. Phishing attacks account for a significant proportion of reported incidents, reflecting attackers' preference for exploiting human vulnerabilities.

Stakeholder	**Impact Type**	**Consequences**
Banks	Financial	Revenue loss, recovery costs
Customers	Personal	Identity theft, monetary loss
Regulators	Legal	Compliance enforcement
Economy	Systemic	Reduced trust in digital finance

Malware-based attacks are often associated with advanced persistent threats, indicating a high level of sophistication among cybercriminals. The analysis also highlights a correlation between user awareness and susceptibility to cyber attacks. Customers who lack basic cyber security knowledge are more likely to fall victim to fraud. From an organisational perspective, banks that invest in advanced security technologies and employee training demonstrate greater resilience against cyber threats. However, the analysis indicates that technological measures alone are insufficient without strong governance and user education. The discussion underscores the importance of a multi-layered security approach that integrates technical, organisational, and behavioural measures. Continuous monitoring and timely response to incidents are crucial for minimising the impact of cyber attacks.

Risk Mitigation Strategies and Security Measures

Effective mitigation of cyber security risks in online banking requires a comprehensive strategy encompassing multiple dimensions. Technical measures such as data encryption, secure communication protocols, and intrusion detection systems play a vital role in protecting sensitive information. Multi-factor authentication enhances security by requiring users to provide additional verification beyond passwords. Organisational measures include the development of robust security policies, regular security audits, and incident response planning. Employee training programmes are essential to prevent insider threats and ensure adherence to security best practices.

Security Measure	**Purpose**	**Effectiveness**
Encryption	Data protection	High
Multi-factor authentication	Access control	Very High
Firewalls & IDS	Threat detection	High
User awareness training	Behavioural risk reduction	Medium–High
AI-based monitoring	Fraud detection	Very High

At the user level, awareness and education are critical. Customers should be encouraged to use strong passwords, avoid suspicious links, and regularly update their devices. Banks can support users by providing timely alerts and guidance on safe online banking practices.

Emerging technologies such as artificial intelligence and machine learning offer promising solutions for real-time threat detection and fraud prevention. By analysing transaction patterns, these technologies can identify anomalies and prevent fraudulent activities more effectively.

Role of Regulations and Compliance

Regulatory frameworks play a crucial role in strengthening cyber security in the banking sector. Compliance with established standards ensures that banks adopt minimum security requirements and follow best practices. Regulations often mandate risk assessments, data protection measures, and incident reporting mechanisms. Compliance not only enhances security but also builds customer trust and confidence in online banking services.

However, regulatory compliance should be viewed as a baseline rather than a comprehensive solution. Banks must go beyond compliance requirements to address emerging threats and adopt innovative security solutions. Collaboration between regulators, banks, and technology providers is essential for creating a resilient cyber security ecosystem.

Conclusion

The study highlights the growing significance of cyber security risks in online banking and their potential impact on financial stability and customer trust. As online banking continues to expand, cyber threats are becoming increasingly sophisticated and persistent.

The analysis demonstrates that cyber security risks arise from a combination of technological vulnerabilities and human factors. Addressing these risks requires a holistic approach that integrates advanced security technologies, organisational policies, regulatory compliance, and user awareness. By adopting proactive risk management strategies and continuously evolving security measures, banks can effectively mitigate cyber threats and ensure secure online banking services. The study underscores the importance of collective efforts by banks, regulators, and customers in safeguarding the digital financial ecosystem.

Future Scope

Future research can focus on empirical studies involving customer surveys and experimental analysis of security mechanisms. The integration of artificial intelligence and blockchain technologies in online banking security presents significant research opportunities.

Additionally, studies examining cross-country regulatory frameworks and their effectiveness in mitigating cyber risks would provide valuable insights. As cyber threats continue to evolve, continuous research and innovation are essential for ensuring the long-term security and resilience of online banking systems.

REFERENCES

1. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
2. Basel Committee on Banking Supervision. (2021). *Cyber-resilience: Range of practices*. Bank for International Settlements.
3. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Computers & Security*, 87, 101589. https://doi.org/10.1016/j.cose.2019.101589
4. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426
5. Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware analysis techniques and tools. *ACM Computing Surveys*, 44(2), 1–42. https://doi.org/10.1145/2089125.2089126
6. ENISA. (2022). *Threat landscape for the financial sector*. European Union Agency for Cybersecurity.
7. Florêncio, D., & Herley, C. (2019). Phishing and money mules. *IEEE Security & Privacy*, 17(1), 28–35. https://doi.org/10.1109/MSEC.2018.2885862
8. Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2018). Analysis of unintentional insider threats. *IEEE Security & Privacy*, 16(2), 45–54. https://doi.org/10.1109/MSP.2018.1870878
9. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
10. Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197
11. ISO/IEC. (2018). *ISO/IEC 27001: Information security management systems — Requirements*. International Organization for Standardization.

12. Kshetri, N. (2018). Cybersecurity and cyberwar: What everyone needs to know. *Journal of Cybersecurity*, 4(1), 1–10. https://doi.org/10.1093/cybsec/tyy012
13. Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16th ed.). Pearson.
14. OECD. (2020). *Digital security risk management for economic and social prosperity*. OECD Publishing.
15. RBI. (2021). *Cyber security framework for banks in India*. Reserve Bank of India.
16. Sharma, A., & Mathur, S. (2021). Artificial intelligence-based fraud detection in online banking systems. *International Journal of Information Security*, 20(4), 527–540. https://doi.org/10.1007/s10207-020-00520-6
17. Stallings, W. (2020). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.
18. Symantec. (2021). *Internet security threat report*. Broadcom Inc.
19. Verizon. (2023). *Data breach investigations report*. Verizon Enterprise.
20. Alasmary, W., Alhaidari, F., Alshdadi, A., & Mahmoud, A. (2019). Cybersecurity challenges in the financial services sector. *Future Generation Computer Systems*, 95, 109–120. https://doi.org/10.1016/j.future.2019.01.023