IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 15, Issue 7, July 2025, ||Series -1|| PP 01-09

An Integrative Review of Cybersecurity Trends, Threats, And Safeguards in the Banking Sector of Bangladesh

MD. MAMUNUR RASHID,
(General Manager, Bangladesh Krishi Bank). Corresponding Author
Email: mamun2008@ymail.com
Received 02 July 2025; Accepted 12 July 2025

Abstract
The digital transformation of Bangladesh's banking system, driven by FinTech innovations and online services, has significantly improved the conditions of financial accessibility and inclusion. However, this advancement has also highlighted the sector's vulnerability to a wide range of cyber threats, including phishing, ransomware, hacking, and insider attacks. Many banks operate with old legacy systems, inadequate infrastructure, outdated regulations, and a shortage of skilled cybersecurity professionals, making them exposed to major digital risks. This study adopts an integrative review approach to analyze the inherent trends, threats, and safeguards related to cybersecurity in the Bangladeshi banking ecosystem. It also elucidated the findings from academic publications, industry reports, and policy documents to present a comprehensive understanding of the current cybersecurity landscape in the Bangladeshi banking sector. The research depicted the key challenges such as regulatory gaps, institutional weaknesses, technological deficiencies, and human-centric risks. To demonstrate these issues, the study proposes a multifaceted safeguard framework consisting of technological solutions (AI-based monitoring, encryption, blockchain), institutional reforms (policy enforcement, audits, public-private partnerships), and human-centered strategies (awareness training, ethical practices). By incorporating insights from multiple disciplines, this paper offers rational guidance for policymakers, practitioners, and researchers working to advance cybersecurity in the emerging economies of Bangladesh.
Keywords: *Banking System, FinTech, Cybersecurity, Cyber Threats, Cyber Safeguards, Risk Management*

I. Introduction and Background

Bangladesh has experienced remarkable growth and transformation in the banking sector over the last decades, largely driven by emerging banking digitalization and financial technology (FinTech) integration (Raghavendra, 2023). The emergence of online banking, mobile banking, ATMs, and online financial services is now available to customers in remote corners more efficiently and with greater convenience than ever before in Bangladesh. This progress has not only improved accessibility to banking services for the masses but has also acted as a key role player in economic development and financial inclusion throughout the country (Rahman, 2022). This paradigm shift of digitization has imposed a new set of complexity, pressure, and challenges, particularly from the perspective of cybersecurity. Banking activities are more dependent on digital infrastructures. So, they become more exposed to cyberwarfare. In recent times, some examples of incidents such as data breaches, ransomware, phishing, identity theft, and financial fraud have become common in Bangladesh (Saeed et al., 2023). Bangladeshi banks have also faced many threats to their cyberspace and infrastructure, including high-profile incidents (Zahoor et al., 2016). For example, the 2016 Bangladesh Bank heist was an example of the serious consequences of inadequate cybersecurity practices in the financial sector. Despite increasing awareness of cybersecurity-related issues among banking institutions and executive bodies in Bangladesh, the current realm of academic research on this topic related to the cybersecurity of the banking sector remains fragmented and segregated. There are a lot of existing studies that focus on incoherent aspects of cybersecurity, such as technical solutions, risk management frameworks, or specific types of cyberattacks (Khan and Barua, 2009; Sikder and Islam, 2023; Joveda et al., 2019). Very few studies offer a pragmatic view that connects emerging cyber threats, trends, and the corresponding safeguards needed to save the banking system in an interdisciplinary and policy-oriented manner. This integrative review tried to bridge that gap by underscoring a wide range of present pieces of literature on the cybersecurity landscape of the banking sector in Bangladesh. The aim is to identify relevant trends in cyber threats, scrutinize the types of risks currently faced by banks, and illustrate the appropriate safeguards that can be implemented at the institutional and systemic levels. The things that distinguish this study from previous research are its multidisciplinary approach arising from cybersecurity, banking, policy, and technological perspectives to a holistic understanding of the current situation in banking. Moreover, this research will make efforts to subscribe to the growing field of digital risk management in developing economies and support efforts to build a more resilient and secure financial banking infrastructure in Bangladesh. Furthermore,

the findings from diverse literature and research sources, including academic papers, government publications, industry reports, cases, monographs, and theses, this study aims to contribute to both practitioners and policymakers. It provided valuable insights that can guide future cybersecurity strategies, investments, and regulations that enrich the unique context of Bangladesh's banking ecosystem. As cyber threats continue to grow in large numbers, this research illustrates the necessity of urgent, proactive, collaborative efforts from banks, regulators, and technology providers to protect customers and users, maintain customer trust, and ensure the stability of the economic system for Bangladesh.

1.1 Research Objectives

The research goal is to elucidate the cybersecurity trends, threats, and safeguards in the banking sector of Bangladesh.

The specific objectives are

1. To identify the cybersecurity trends and threats for the banking sector of Bangladesh.
2. To illustrate the possible safeguards against these security threats for the Bangladeshi banking system

II. Materials and Methods

This study applied an integrative literature review methodology to explore and analyze cybersecurity trends, threats, and safeguards from the perspective of the Bangladeshi banking sector. Among the various literature review approaches, systematic, semi-systematic, and integrative, the integrative review was chosen for its ability to synthesize knowledge across multiple disciplines, including information technology, finance, policy, and human behavior (Snyder, 2019). This methodology is particularly appropriate for complex and evolving issues like cybersecurity, where empirical studies, conceptual papers, policy discourses, and case studies all contribute to a comprehensive understanding of a study.

2.1 Research Design

A literature review can be a research study (Snyder, 2019). In this research, Snyder's (2019) approach was adopted. The research followed a structured four-stage process:

1. Design
2. Literature Collection
3. Thematic Analysis
4. Synthesis and Reporting

In the first stage, "design phase", the research questions and objectives were constructed to investigate three key domains: cybersecurity trends in the banking sector, major threats faced by Bangladeshi banks, and potential safeguard strategies. The goal was to generate a conceptual framework that intersects these dimensions in a coherent and actionable model.

2.2 Data Collection

The literature collection phase consists of selecting peer-reviewed journal articles, conference papers, government reports, news articles, industry white papers, and policy documents. Databases included in this research were Google Scholar, Scopus, Web of Science, and Elsevier. Specific keywords for searching papers, such as cybersecurity in banking, FinTech threats, Bangladesh banking system, phishing, ransomware, "ICT Act in Bangladesh, and Digital Security Act in Bangladesh," were used to filter the appropriate studies for this research. Both recent publications (2010–2025) and foundational documents were stored to ensure the historical context and current situation of banking in Bangladesh.

Over 40 high-quality sources were collected, with a focus on Bangladesh-specific cybersecurity issues, regulatory frameworks, and sector-specific vulnerabilities. Priority was given to an article that discussed cybersecurity from a multidisciplinary perspective, demonstrating technical, legal, and human elements.

2.3 Data Analysis

A qualitative content analysis was adopted to extract themes and patterns from the collected literature. No primary data collection was conducted in this study, and the depth of the literature enabled a comprehensive thematic analysis. Thematic coding was applied to scrutinize the key recurring themes such as phishing and social engineering, data protection practices, regulatory gaps, insider threats, AI-based safeguards, and institutional audit mechanisms (Clarke and Braun, 2016). These themes were then incorporated into the research objectives to ensure consistency with the conceptual framework (Kiger and Varpio, 2020).

Where applicable, some examples of quantitative data, such as statistics on malware attacks, financial losses, and user awareness levels (from survey reports and national databases) were also incorporated to support the qualitative findings. This mixed use of data types enhanced the validity of the analysis.

2.4 Ethical Considerations

As this study is totally based on secondary data from online available sources, ethical approval was not required. However, all sources were cited properly, and the researcher showed how all the parts of the review were completed. All credible and valid publications were given importance to maintain academic integrity. The result of this methodological process is a theoretical conceptual framework that links digital banking components with cybersecurity trends, threats, and recommended safeguards in the last part. This framework depicts the coherent realities in Bangladesh's current banking sector. Besides that, it proposes a holistic and adaptive strategy for future Cybersecurity in banking sector planning.

The integrative literature review method is extensively applied in the field of research presently like see (Sajib, 2025); in transport study, (Shahjahan and Sajib, 2021); as a main research methodology, (Sajib and Shahjahan, 2022); as the main research methodology.

Table 1.1 Collection of Studies Collected for Conducting this Study

Themes	Databases Source	Citation
Cybersecurity Awareness & Training, Insider Threats, Incident Response and Recovery, Risk Assessment Practices, Network & Endpoint Security Measures, Data Protection Practices, High rates of malware, phishing, spam, Encryption, Data Loss Prevention (DLP), and policies to safeguard sensitive banking data, Negligence and intentional data leaks by insiders	Google Scholar	(Sikder, 2016)
Atm Fraud, Ransomware, Phishing, Data Breaches,	Google Scholar	(Hossain et al., 2025)
Money Laundering, Reputational Risk, Financial Losses, Fake shipping Documents,	Google Scholar	(Joveda et al., 2019)
Outdated Technology, Lack of Awareness, Insufficient Investment, Lack of Smart Cities and IoT, Cloud Computing, DDoS Attacks, Strict Regulation, and International Collaborations	Google Scholar	(Rahman, 2022)
Behavioral Changes, Social Engineering, Malware Attack, Insider Threats	Google Scholar	(Rihan, 2023)
Ransomware, Data Breaches, Robust Defense,	Google Scholar	(Best, et al., 2019)
Existing Laws (ICT ACT, Digital Security ACT), Lack of Awareness, Compatible Stakeholders, Emerging Technology, AI, Blockchain, Cross-border Operations,	Google Scholar	(Hasan and Hossain, nd)
Regulatory and Legal Gaps, Lack of Legal Sector Preparedness, Multi-Stakeholder Coordination, Zero Trust, and AI-Based Safeguards	Google Scholar	(Sikder & Islam, 2023)
Pirated Software,	Google Scholar	(Nabi and Islam, 2014)
Smishing, Malware, Cyberbullying,		(Abbas, 2022)
Cyber Bullying,	Google Scholar	(Paul, 2022)
Women Victimization, Human Violation, Data Localizations, Prejudice	Google Scholar	(Siddique, 2019)
Cyber Attacks, Cyber Security Measures DSA,	Google Scholar	(Zahoor et al., 2016)
Digital Development, Wiretapping, Surveillance	Google Scholar	(Sijan et al, 2022)
Comprehensive CyberSecurity Legislation, AI Threat Detection, Blockchain, Quantum Encryption,	Google Scholar	(Sayduzzaman et al., 2024)
ATM Fraud, Banking Scams, Money Laundering, Lack of Skills in Professionals	Google Scholar	(Khan and Barua, 2009)
AI, Encryptions, Real Monitoring Tools, Lack of Firewalls, IT Experts,		(AI Mahmud, et al, 2025)
Gender Diversity, Board Interdependence, Voluntary Disclosure, Insider Domination	Google Scholar	(Mazumder and Hossain, 2022)
State Sponsored Attack, Dependency on foreign Services, Data Theft, Dual Criminality Issues, Social Stigma, Hacking, ICT ACT 2006, ICT Awareness,	Google Scholar	(Bonnya, 2020)
Bangladeshi Laws, Cyber Security Acts	Google Scholar	(Chaki et al, 2024)
Next Generation Solution, Quantum Resistant Cryptography,	Google Scholar	(Manduru, 2018)
Convenience vs Security Trade-off	Google Scholar	(Raghavendra, 2023)
Systemic Flaws,	Springer Nature	(Babu et al., 2025)
Challenges in Cyber Security	Scopus, Web of Science	(Saeed et al., 2023)
Data Privacy, Customer Security, Legacy System, Compliance Management, Vendor Risk Management, Robust Data Privacy, Data Encryption, Employee Training	Scopus	(Wang et al., 2024)
Data Defense Strategy, Cyber Security Future Paradigm, Data Breaches,	Scopus, Google Scholar	(Biplob et al., 2024)

III. Conceptual Frameworks

This research scheme is more clarified with the following conceptual framework.

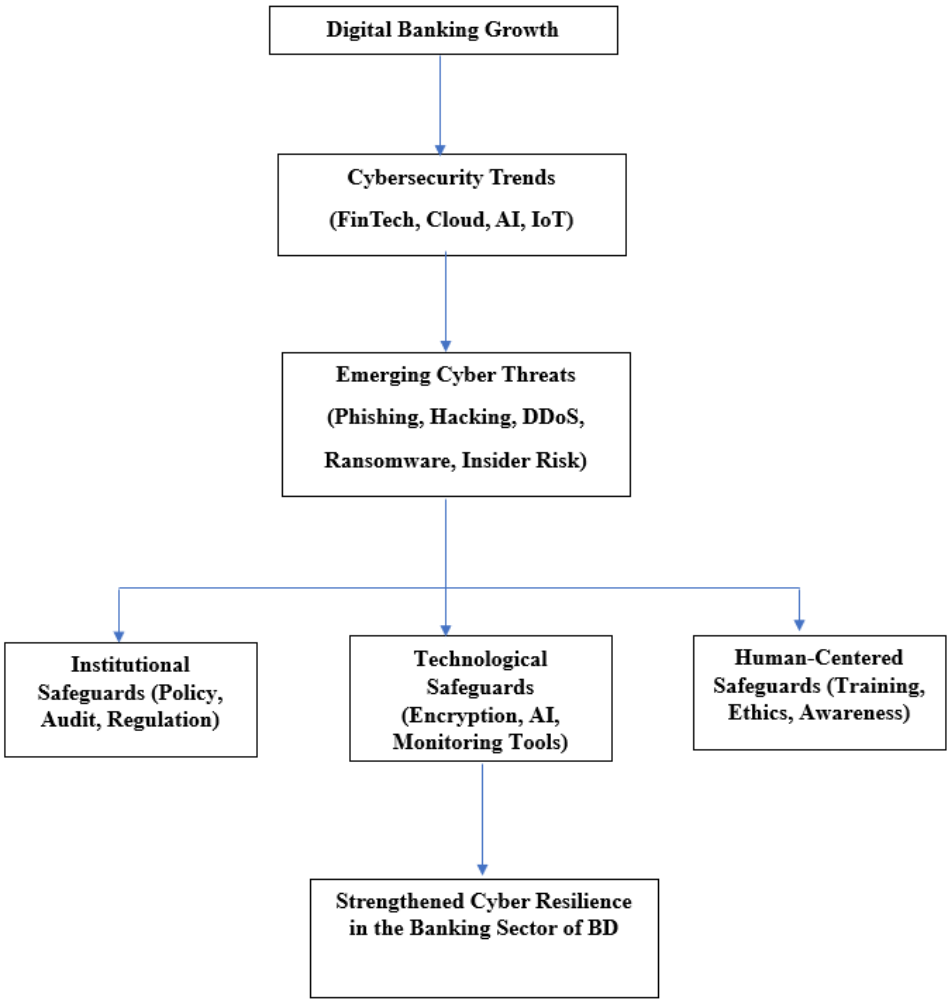

Figure 1.1: How Threats, Trends, and Safeguards are Conceptualized in this Study

The above conceptual framework depicts the multifaceted relationship between digital transformation and cybersecurity in Bangladesh's banking sector, generated from secondary literature. It begins with Digital Banking Growth, which is accelerated by technology and innovations, for example: FinTech, cloud computing, artificial intelligence (AI), and the Internet of Things (IoT). These technological innovations enhance accessibility and efficiency for the users and stakeholders and also introduce new vulnerabilities. As a result, Emerging Cyber Threats like phishing, hacking, ransomware, DDoS attacks, and insider risks are emerging in Bangladesh. These threats originate from both external attackers and internal system or personnel weaknesses.

To reduce these threats, this conceptual framework proposes a three-tiered safeguard strategy. They are

1. Institutional Safeguards: They are regulatory policies, legal audits, and oversight mechanisms designed to maintain compliance and enhance the sector's readiness.
2. Technological Safeguards: Including encryption, AI-driven threat detection, and continuous monitoring tools, these measures execute secure digital systems and sensitive financial data. The third one is
3. Human-Centered Safeguards: Including training, ethics, and cybersecurity awareness among employees and customers to reduce human errors and insider threats.

These components interact collaboratively to build a Strengthened Cyberspace in Bangladesh's banking sector, making it withstand, respond to, and recover from cyber warfare more effectively.

IV. Results

Key cyber threats identified include phishing, ransomware, DDoS attacks, ATM fraud, insider threats, and systemic vulnerabilities from outdated infrastructure and regulatory gaps, with an integrative literature review method. Besides, this study demonstrates a multidisciplinary framework for safeguards in technological,

institutional, and human-centered systems. For Technological, advanced encryption, AI-driven monitoring, and blockchain for secure transactions. For Institutional, the updated regulations, public-private partnerships, and robust incident response plans. And for Human-Centered, Employee/customer training, ethical policies, and addressing skill gaps in the banking sector of Bangladesh. The findings urged collaborative efforts among banks, regulators, international bodies, and other stakeholders to strengthen cyber resiliency and ensure financial security and stability for Bangladesh.

4.1 Discussions

The findings of this study demonstrated the multifaceted nature of cybersecurity challenges encountered by the banking sector of Bangladesh. It also seeks urgent initiatives for comprehensive safeguards in this sector. The below sections synthesize the identified trends, threats, and safeguards while setting them within the broader landscape of digital banking growth, regulatory frameworks, and technological advancements for Bangladesh. Moreover, they were discussed from the perspective of a future technological paradigm shift for the banking system of Bangladesh.

4.2 Trends of Cybersecurity Aspect in Banking Sectors of Bangladesh

The growing digitization of banking activities in Bangladesh, executed by FinTech innovations, cloud computing, and AI, has significantly improved accessibility, effectiveness, and convenience for customers and banking users. However, this digital transition has also created compounded vulnerabilities for them. This study identified several key trends, like emerging technologies applications. Technologies such as AI, blockchain, and IoT are being incorporated into banking operations, but their establishment often surpasses the demarcation of strict security protocols (Rahman 2022; Sayduzzaman et al., 2024). A rise in Dependency on cross-border operations is now apparent. Illegal national/International transactions bring banks to international cyber threats, such as state-sponsored attacks and dual criminality issues (Rahman, 2022). The shift to online banking and remote electronic transactions has proliferated the possibility of attacks from cybercriminals, with phishing, smishing, and malware attacks (Sikder, 2016). These incidents are becoming more prevalent day by day in Bangladesh. These trends put them in a fixed situation of digital banking while fostering financial inclusion and economic growth. It also poses systemic risks if cybersecurity measures cannot cope with technological adoption and progress.

4.3 Significant Cyber Threats

The analysis categorizes a wide range of cyber threats pointing to Bangladeshi banking sectors, which can be categorized as follows:

4.4 Technical Threats

Phishing and Social Engineering: These are the most common attack vectors, harming human vulnerabilities to gain unauthorized access to sensitive personal information. This sensitive information is often viral in cyberspace.

Ransomware and DDoS Attacks: One of the high-profile incidents was the 2016 Bangladesh Bank heist. It demonstrated the horrific financial consequences in the history of Bangladesh (Zahoor et al., 2016). This incident can compare the place of Bangladesh with other countries from the global south in the banking system.

ATM Fraud and Data Breaches: Older technology and poor encryption protocols make ATMs and financial transactional systems easy targets for skimmers and data theft (Hossain et al., 2025; Sikder, 2016; Siddique, 2019; Bonnya, 2020). The victims are poor and illiterate, vulnerable communities.

4.5 Institutional Threats and Human-Centric Intimidation

Insider threats like negligence, data leaks, and lack of cybersecurity awareness among administrators contribute significantly to security breaches. The regulatory gaps inconsistent with the enforcement of existing laws (e.g., ICT Act, Digital Security Act) and the deficiency of skilled cybersecurity professionals extend the vulnerabilities (Hasan and Hossain, nd; Bonnya, 2020). This vulnerability puts the banking customer into a more complex situation where they can not solve their own problem without expert help.

4.6 Systemic and Cross-Cutting Threats

The Dependency on Foreign Services, like third-party vendors, for critical infrastructure (e.g., SWIFT systems) can introduce risks of supply chain attacks. The pirated software and outdated systems make widespread use of unlicensed software and legacy systems. These usages leave banks vulnerable to unpatched vulnerabilities (Nabi and Islam, 2014). These threats often intersect, creating compounded risks for the banking system. For example, a phishing attack can lead to a ransomware infection, which might then hinder the weak network security to exfiltrate data (Best et al., 2019).

4.7 Proposed Safeguards

To reduce the threats, this study proposes a comprehensive framework combining technological, institutional, and human-centered safeguards. They are elucidated below:

4.8 Technological Safeguards

Advanced Encryption and AI-based monitoring, like implementing quantum-resistant cryptography and real-time AI-driven threat detection, can enhance data protection (Manduru, 2018). The Blockchain for secure transactions can distribute a ledger technology system that could reduce fraud in cross-border banking operations and improve transactional transparency (Hasan and Hossain, nd). The endpoint and network security can deploy the next-generation firewalls and regular system updates to protect against malware and DDoS attacks (Rahman, 2022). This protocol can reduce risk for banking customers.

4.9 Institutional Safeguards

Strengthening regulatory frameworks, policymakers must update cybersecurity laws to depict emerging threats and ensure compliance through audits and penalties in Bangladesh. Public-private partnerships with the collaboration among banks, regulators, and international bodies (e.g., INTERPOL) can simplify knowledge sharing and resource pooling (Rahman, 2022). Response Plans in banking need robust protocols for rapid recovery from breaches, including forensic analysis and customer notification systems (Wang et al., 2024). Thus, banking sectors can strengthen institutional safeguards.

4.10 Human-Centered Safeguards

Here, cybersecurity training programs are intrinsic to Cybersecurity development. Regular workshops and simulations to train employees and customers about phishing, social engineering, and safe online practices are vital. There should be ethical and Inclusive Policies (Wang et al., 2024; Sikder, 2016). Addressing gender disparities in cybersecurity roles and promoting a culture of accountability within organizations can make Cybersecurity more viable. The ethics, norms, and values are important here. We must realize what we should do and not do in cyberspace.

4.11 Solutions and Implications

This study proposes a combination of strategic, technological, institutional, and human-centered recommendations for improving the banking sector of Bangladesh. They are vital to creating a secure, resilient, and globally oriented digital banking ecosystem in Bangladesh by eradicating cyberattacks and cybercrime. In doing so, we must modernize our banking infrastructure. The base step in ensuring safety in the banking sector is to upgrade legacy systems and IT infrastructure. A large number of financial institutions still rely on obsolete hardware and cracked software, which are highly vulnerable to malware and other forms of cyber trespass (Biplob et al., 2024). So, banks must have robust security with design principles in system architecture, regular software updates, and vulnerability patching mechanisms. Advanced authentication tools are also needed, such as biometric and multifactor authentication (MFA). There should be Cutting-Edge Technological Solutions (Saeed et al., 2023). Fighting against sophisticated threats, banks must endorse advanced cybersecurity technologies (Rihan, 2022). Here, Quantum Resistant Cryptography can ensure the future-proof sensitive data against emerging decryption threats. AI-Based Threat Detection Systems and Machine learning algorithms can scrutinize the anomalies in real time, detecting phishing attempts, malware behavior, or data exfiltration (Wang et al., 2024). So, they are effective here. Blockchain Integration can implement blockchain-based transaction systems for improved transparency and fraud reduction, especially in cross-border and global operations (Hasan and Hossain, nd). Zero Trust Architecture can make a transition from perimeter-based defenses to identity-oriented device-based trust mechanisms. Moreover, strengthening legal and regulatory frameworks in existing laws such as the ICT Act (2006) and Digital Security Act (2018) must be amended and updated to address modern cybercrime challenges in Bangladesh (Bonnya, 2020). This change can be achieved through establishing a specialized Cybersecurity Regulatory Authority to investigate compliance. Creating sector-specific cybersecurity policies is also effective (e.g., for banking, insurance, and e-commerce) (Chaki et al., 2024). Mandatory reporting of cyber incidents should be enforced, and conduction of regular audits must be strengthened in the Banking sector, where political interventions should be abolished. The initiatives of cross-border cybercrime prosecution to fight issues like data theft from international sources can be implemented.

Promoting Public-Private Partnerships and International Collaboration across the financial sectors and borders is vital (Sikder and Islam, 2023; Biplob et al., 2024). Fostering public-private partnerships between banks, telecom providers, FinTech, and government agencies can ease the condition. Establishing data-sharing platforms for real-time intelligence on cyber threats is more important than any other initiative. Bangladesh should also join in regional and international initiatives like INTERPOL's Cybercrime Task Forces or APCERT (Asia Pacific CERT) to improve incident response and global alignment to ensure cross-border Cybersecurity (Bonnya, 2020). More investment in human capital and Cybersecurity Awareness can reduce the weakness of people in Cybersecurity. Human error, negligence, and insider threats have extensively led to breaches in Bangladesh's banking sector (Bonnya, 2020). Therefore, cybersecurity training should be made mandatory for all banking employees, from IT staff to front-desk officers. Cyber hygiene awareness campaigns must be arranged for banking

customers, especially for new customers in digital banking. Cybersecurity education should be institutionalized in the university curriculum and promote ethical hacking and cybersecurity certification programs to build local talent in this sector (Sikder, 2016; Wang et al., 2024). Ensuring ethical and inclusive Cybersecurity practices will benefit the financial services. There should be gender-sensitive policies, and this sector should promote equal participation of women in cybersecurity roles, addressing current imbalances. Ethics in AI policies must be ensured (Hossain et al., 2025). The automated systems should respect privacy, and fairness as well as not discriminate against any groups or communities. With Cybersecurity training and inclusive mechanisms, we can bridge the Digital Divide and Technological Disparities. The urban-rural digital divide can be an outcome of unequal exposure to cyber threats that can be tackled with Cybersecurity (Rahman, 2022). Improvement in internet infrastructure in rural areas with secure access protocols is also possible with it. Providing financial literacy and digital banking training for underserved populations is mandatory to enhance Cybersecurity (Biplob et al., 2024). Subsidized secure devices or banking kiosks in remote regions can help implement inclusiveness. All banking and financial institutions must have documented, tested, and regularly updated incident response plans. They should include steps for detection, isolation, containment, mitigation, and recovery. Running annual penetration testing and red-team-blue-team simulations can be effective here (Best et al., 2019). Ensuring business continuity and disaster recovery planning are integrated with cybersecurity frameworks can control the negative consequences (Paul, 2022). To tackle enforced vendor risk and compliance management, banks must examine the security posture of third-party vendors and service providers. Developing vendor assessment frameworks with signed service-level agreements (SLAs) that include cybersecurity clauses is the first necessary step (Manduru, 2018). Conducting regular security audits of vendors, especially those handling sensitive banking data, should be ensured properly. Thus, the continuous monitoring and evaluation in the banking sector of Bangladesh can change the system forever. Cybersecurity is not a one-time investment. It is a continuous process (Nabi and Islam, 2014). Setting up Security Operation Centers (SOCs) with 24/7 threat monitoring capabilities, using real-time dashboards and metrics to measure cybersecurity performance, and updating cybersecurity policies regularly based on threat intelligence and risk assessments are also determining components to tackle the banking safeguards in Cybersecurity for Bangladesh.

These recommendations assert a multidisciplinary and collaborative approach, involving not just financial institutions but also regulators, policymakers, academia, and citizens. When technology offers tools, it is the strategic alignment with human empowerment that ultimately determines the future of cybersecurity for Bangladesh. By following these recommendations, Bangladesh can build a strong cybersecurity ecosystem in the banking sector. Thus, the safeguard in Cybersecurity will protect the economy, institutions, and citizens from emerging digital and technological threats.

V. Conclusions and Recommendations

The escalating cybersecurity risks in Bangladesh's banking sector, driven by digital expansion and global interconnectedness, have been scrutinized in this study. The paradoxical scenario is that while technological advancements like FinTech and AI have revolutionized banking services, they have also institutionalized systemic flaws and vulnerabilities. The 2016 Central Bank heist is an example of these catastrophic consequences. Inadequate safeguards expose this sector to sophisticated threats such as ransomware, phishing, fraud, and insider leaks. The analysis conducted in this study identified three emerging gaps 1. Technological lag, which is an outdated system and is largely dependent on unlicensed software, hinders robust defenses.

2. Regulatory Shortcomings, which are existing laws (e.g., ICT Act) that lack enforcement mechanisms to address evolving threats. 3. Human Factors is another one. Insufficient training and awareness perpetuate cyber risks, compounded by a shortage of skilled professionals.

To moderate these challenges, the study advocated for a comprehensive framework integrating technology, policy, and human capital. Besides, adopting cutting-edge solutions is necessary. Quantum-resistant cryptography and AI-based threat detection to future-proof systems is this kind of cutting-edge solution. There should be more collaborative mechanisms. Public-private partnerships. Prioritizing Education at the Nationwide level of cybersecurity training programs and ethical guidelines to foster a culture of accountability is also important. The study's interdisciplinary scheme bridges gaps in existing research by linking cyber threats with practical safeguards relevant to Bangladesh's unique context. However, the prevailing in the proactive investment in infrastructure, stricter regulatory oversight, and inclusive policies to address digital divides. As cyber threats evolve, the banking sector must apply adaptive strategies to safeguard economic stability and maintain public trust nationwide. Ultimately, this research is conducted to provoke policymakers, financial institutions, and technology providers to collaboratively build a resilient cybersecurity ecosystem—one that balances technology with imperatives of security and equality in future Bangladesh's banking system. There are a lot of studies related to this topic in Bangladesh. However, this study is different from other research in that direction of combining the electronic trends of threats together for the banking sector of Bangladesh. Besides, it will propose possible safeguards based on the identified threats to the banking system of Bangladesh, which is still not mentioned in

any research at the same time. Thus, the fintech and multidisciplinary paradigm of cybersecurity and banking sectors will be facilitated through this study. So, first of all, Bangladesh must develop an IT infrastructure system to fight against cyberattacks. All the stakeholders related to Cybersecurity must be trained at the pace of global standards. Global collaboration must be strengthened. Regional assistance and agreement amongst the neighboring countries can ease the Cybersecurity risk by bringing the convicts under jurisdiction. Digital divide and other technological discrimination can lead to more cybercrime. So, they should be abolished.

Declaration

The researcher has no conflict of interest or economic interest except academic interest for this study.

References

[1]. Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat to banking industries in Bangladesh: in quest of an effective legal framework and cybersecurity of financial information. International Journal of Economics and Finance, 11(10), 54-65.

[2]. Rahaman, M. M. (2022). Recent advancement of cybersecurity: Challenges and future trends in Bangladesh. Saudi Journal of Engineering and Technology, 7(6), 278-289.

[3]. Rihan, A. The Landscape of Cyber Crime in Bangladesh: Challenges, Trends, and Mitigation Strategies.

[4]. Best, M., Krumov, L., & Bacivarov, I. C. (2019). Cyber Security in the Banking Sector. International Journal of Information Security & Cybercrime, 8(2).

[5]. Hasan, M. R., & Hossain, M. A. A Simplified Cybersecurity Policy Framework for the Financial Institutions in Bangladesh: A Survey of Literature.

[6]. Nabi, M. N., & Islam, M. T. (2014). Cyber Security in the Globalized World: Challenges for Bangladesh. In I. Filipovic, M. Klacmer Calopa, F. Galetic, & Varazdin Development and Entrepreneurship Agency (Eds.), Economic and social development 7th international scientific conference, New York: Book of Proceedings.

[7]. Zahoor, Z., Ud-din, M., & Sunami, K. (2016). Challenges in Privacy and Security in the Banking Sector and Related Countermeasures. International Journal of Computer Applications, 144(3), 24–35. https://doi.org/10.5120/IJCA2016910173

[8]. Siddique, N. A. (2019). A Framework for the Mobilization of Cyber Security and Risk Mitigation of Financial Organizations in Bangladesh: A Case Study.

[9]. Paul, S. (2022, September 19). Bangladesh is at serious risk of cyber crimes. What are we doing wrong? Dhaka Tribune. https://www.dhakatribune.com/bangladesh/2022/12/12/cabinetasks-for-strengthening-cyber-security

[10]. Abbas, M. (2022, December 18). Cyberbullying increases by 20%. The Daily Star. https://www.thedailystar.net/news/bangladesh/crime-justice/news/cyberbullying-increases-203199361

[11]. Sijan, M. A. H., Shahoriar, A., Salimullah, M., Islam, A. S., & Khan, R. H. (2022, March). A review on e-banking security in Bangladesh: An empirical study. In Proceedings of the 2nd International Conference on computing advancements (pp. 330-336).

[12]. Sayduzzaman, M., Sazzad, S., Rahman, M., Rahman, T., & Uddin, M. K. Managing Escalating Cyber Threats: Perspectives and Policy Insights for Bangladesh.

[13]. Khan, M. S., & Barua, S. (2009). The status and threats of information security in the banking sector of Bangladesh: Policies required. Bangladesh Journal of MIS, 1(2).

[14]. Al Mahmud, M. A., Dhar, S. R., Debnath, A., Hassan, M., & Sharmin, S. (2025). Securing Financial Information in the Digital Age: An Overview of Cybersecurity Threat Evaluation in Banking Systems. Journal of Ecohumanism, 4(2), 1508-1517.

[15]. Mazumder, M. M. M., & Hossain, D. M. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? Journal of Accounting in Emerging Economies, 13(2), 217-239.

[16]. Bonnya, M. A. (2020). Cyber Threat and Security: Bangladesh Perspective. IOSR Journal Of Humanities And Social Science (IOSR-JHSS), 25(3), 19-28.

[17]. Chaki, C., & Biswas, A. Inspecting the Legal Aspects of the Cyber Crimes Committed Against Financial Institutions with Special Reference to the Bangladesh Bank Cyber Intrusion.

[18]. Mandru, S. (2018). The Role of Cybersecurity in Protecting Financial Transactions. Journal of Scientific and Engineering Research, 5(3), 503-510.

[19]. Raghavendra, K. (2023). CHALLENGES IN SECURING BANKING SYSTEMS: EMERGING TRENDS, RISKS, AND DEFENSIVE STRATEGIES.

[20]. Babu, KEK., Hongsrisuwan, N., Jahid, A.M., Ullah, M.A., Shuvo, S.D., Shobuj, M.H. (2025). Cybercrime as a Threat to the Commercial Banking Sectors in Bangladesh: A Critical Analysis. In: Jahankhani, H., Issac, B. (eds) Cybersecurity and Human Capabilities Through Symbiotic Artificial Intelligence. ICGS3 2023. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-82031-1_20

[21]. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses: Resilience: Issues and Recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

[22]. Wang, S., Asif, M., Shahzad, M.F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Comput. Secur., 147, 104051.

[23]. Sajib, S. H. (2025). Risk Factors Contributing to Inland Water Transport Passenger Ferry Accidents in Bangladesh. Journal of Safety and Sustainability.

[24]. Kabir, M. S., & Sajib, S. H. (2021). Impact of the COVID-19 pandemic on small entrepreneurship in Bangladesh. Journal of Entrepreneurship and Business Resilience, 4(1), 41-48.

[25]. Shajahan, K. M., & Hossen, S. S. (2022). POVERTY, FOOD SECURITY AND RESILIENCE TO COVID-19 IN BANGLADESH. Journal of Entrepreneurship and Business Resilience, 5(1), 75-82.

[26]. Biplob, M. B., Ahsan, K. M. M., Al Mohaimin Farabi, M. S. K., & Ahmed, A. (2024). From Data Breaches to Defense Strategies: A Study of Cybersecurity Information Systems' Latest Trends and Future Paradigms

[27]. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339

[28]. Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. Medical teacher, 42(8), 846–854. https://doi.org/10.1080/0142159X.2020.1755030

[29]. Clarke, V., & Braun, V. (2016). Thematic analysis. The Journal of Positive Psychology, 12(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613