Web of Scholars: Multidimensional Research Journal
ISSN: 2751-7543
Volume 04 Number 02 (2025)
https://innosci.org/wos

Article

Topic: Exploring the Fintech Landscape & Cybersecurity of the Banking Operations in Bangladesh

Ashraf Shahriar[1]

1. MPF - DU, IFBI - Eastern University
* Correspondence: ashrafssuharto@gmail.com

Abstract: This study explores the evolving fintech landscape and cybersecurity measures within the banking operations of Bangladesh. With the rapid digital transformation in the financial sector, fintech innovations have significantly enhanced banking services, improving accessibility, efficiency, and customer experience. However, these advancements also expose financial institutions to increasing cybersecurity threats, including data breaches, fraud, and cyberattacks, which pose serious risks to operational integrity and consumer trust. Using a mixed-method approach, this research analyzes the current state of fintech adoption, the regulatory environment, and the cybersecurity challenges faced by banks in Bangladesh. The study identifies key trends such as the rise of mobile banking, digital payment systems, blockchain applications, and AI-driven financial services, while also assessing the effectiveness of existing cybersecurity frameworks in mitigating threats. Findings indicate that while fintech adoption is growing rapidly, regulatory gaps, insufficient cybersecurity infrastructure, and a lack of skilled cybersecurity professionals create vulnerabilities within the banking sector. The study suggests that banks should invest in advanced cybersecurity technologies, enhance regulatory compliance, and foster collaboration between financial institutions, regulatory bodies, and technology providers to strengthen digital security. The research provides valuable insights for policymakers, banking professionals, and fintech entrepreneurs to build a more resilient and secure digital banking ecosystem in Bangladesh, ensuring sustainable growth in the era of financial technology.

Keywords: fintech, cyber security, bangladesh, digital, threat, ict, ai, operations, banking

Citation: Shahriar, A. Topic: Exploring the Fintech Landscape & Cybersecurity of the Banking Operations in Bangladesh. Pioneer: Journal of Advanced Research and Scientific Progress 2025, 4(2), 55-64.

Received: 10th Mar 2025
Revised: 21th Mar 2025
Accepted: 02th Apr 2025
Published: 09th Apr 2025

1. Introduction

The financial technology (fintech) sector has rapidly transformed banking operations worldwide, and Bangladesh is no exception. The country's banking industry has witnessed significant digital advancements, driven by increasing smartphone penetration, internet accessibility, and government initiatives promoting financial inclusion. Fintech solutions, such as mobile banking, digital wallets, and blockchain applications, are reshaping the traditional banking model by enhancing efficiency, accessibility, and customer experience . However, these innovations also introduce cybersecurity threats that pose significant risks to financial institutions, businesses, and consumers. Cybersecurity has become a critical concern as banks in Bangladesh embrace digitalization. The rise in cyberattacks, including phishing, ransomware, and data breaches, underscores the need for robust security frameworks. Regulatory bodies, such as the Bangladesh Bank, have introduced policies to strengthen cybersecurity and safeguard sensitive financial data. Despite these efforts, challenges persist, including outdated security systems, lack of awareness, and resource constraints. Addressing these issues requires a comprehensive approach involving technological advancements, regulatory compliance, and collaboration between financial institutions and cybersecurity experts. This study aims to

explore the current fintech landscape in Bangladesh, its impact on banking operations, and the associated cybersecurity challenges. By analyzing existing literature, industry reports, and real-world cases, this paper will provide insights into the future of fintech in Bangladesh and strategies for enhancing cybersecurity in the banking sector.

LITERATURE REVIEW

Fintech adoption in Bangladesh has accelerated due to the rise of mobile banking, digital payment systems, and online financial services. The growing dependence on fintech solutions has increased cybersecurity vulnerabilities in the banking sector. Several studies highlight the rise of cyber threats, including phishing attacks, malware, and data breaches [1]. Bangladesh Bank has implemented various regulations to enhance cybersecurity in banking operations. The ICT Security Guidelines for Banks and Financial Institutions [2] outlines key security protocols, including data protection measures, incident response mechanisms, and cybersecurity training for employees. Despite the challenges, the fintech sector in Bangladesh presents significant growth potential. Experts suggest that increased investment in cybersecurity infrastructure, public-private partnerships, and customer awareness campaigns can enhance security and foster fintech growth [3]. The integration of emerging technologies like biometric authentication, AI-driven fraud detection, and decentralized finance may further secure banking operations [4].

A. Research objectives:

The primary objectives of this research are to examine the fintech landscape and cybersecurity challenges in Bangladesh's banking sector. These objectives focus on understanding the role of fintech in banking operations, identifying cybersecurity threats, evaluating regulatory frameworks, and exploring future opportunities for a secure digital financial ecosystem.

The secondary objectives to gain a deeper understanding of the fintech landscape and cybersecurity challenges in the banking operations of Bangladesh. These objectives focus on identifying industry-specific trends, consumer behavior, and best practices for securing financial institutions.

B. Application of the dependent and independent variables

In this research, independent variables influence or drive changes, while dependent variables are the outcomes or effects being studied.

C. Hypotheses (H) expansion

H1: The adoption of fintech solutions has a significant positive impact

H2: The growth of fintech services contributes to greater financial inclusion

H3: Consumer trust in fintech services positively influences the adoption of digital banking

H4: Increased fintech adoption leads to a higher risk of cybersecurity threats

H5: Implementing robust cybersecurity measures significantly reduces the risk of financial fraud and cyberattacks in banking operations.

H6: Non-compliance with cybersecurity regulations increases the vulnerability of banks to cyber threats.

H7: A well-defined regulatory framework positively influences the security and stability

H8: Insufficient legal enforcement and regulatory gaps increase cybersecurity risks

H9: Higher digital literacy positively influences the adoption of fintech

H10: Consumer concerns about data privacy and cybersecurity risks negatively impact fintech adoption.

H11: Artificial intelligence and blockchain technology significantly enhance banking security and fraud detection.

H12: Emerging cyber threats, AI-powered attacks, deepfake fraud pose significant risks to the fintech ecosystem.

D. Research Gap

Despite the growing adoption of fintech solutions and increasing focus on cybersecurity in banking operations, several research gaps exist that require further investigation. These gaps highlight areas where existing studies are either insufficient, outdated, or do not fully address critical challenges in the Bangladeshi context.

1. Limited Research on the Integration of Fintech and Cybersecurity in Bangladesh
   - While there are studies on fintech adoption [5] and cybersecurity threats in banking, few studies examine how fintech innovation and cybersecurity measures interact in the financial sector [6], [7]. There is no comprehensive model analyzing the trade-off between fintech growth and cybersecurity risk in Bangladesh's banking industry.
   - Gap: Lack of research on the interdependency between fintech expansion and cybersecurity resilience.
2. Inadequate Analysis of Regulatory Effectiveness in Bangladesh's Fintech Sector
   - The Bangladesh Bank ICT Security Guidelines [8] provide regulatory measures, but there is little research on their effectiveness, enforcement, and compliance levels. Studies such as Khan & Rahman [9] discuss regulatory challenges, but there is limited empirical evidence on the impact of fintech regulations on cybersecurity and banking stability.
   - Gap: Lack of empirical studies assessing the real-world impact of fintech regulations on banking security in Bangladesh.
3. Insufficient Studies on Consumer Trust and Cybersecurity Awareness in Fintech Adoption
   - Islam et al. and Hasan et al. discuss fintech adoption but do not fully explore how cybersecurity concerns affect customer trust and usage of fintech services [10], [11]. There is limited research on customer digital literacy, perceptions of fintech security, and willingness to adopt fintech-based banking solutions.
   - Gap: Need for studies on the relationship between consumer trust, cybersecurity concerns, and fintech adoption.
4. Lack of Research on Cybersecurity Threat Trends in Fintech-Enabled Banking Operations
   - Ahmed & Hossain discuss cybersecurity threats but do not analyze emerging threats such as AI-powered fraud, deepfake scams, and data breaches in digital banking. Studies on ransomware, phishing attacks, and hacking incidents are outdated and do not account for new vulnerabilities introduced by fintech innovations like blockchain, AI, and open banking [12].
   - Gap: Absence of research focusing on new-age cyber threats targeting Bangladesh's fintech sector.
5. Minimal Comparative Analysis Between Bangladesh and Other Emerging Markets
   - Most existing research focuses only on Bangladesh, without comparing it to similar fintech ecosystems in South Asia (e.g., India, Indonesia) or other developing economies. World Bank provides a regional overview of digital finance but does not analyze how Bangladesh's fintech cybersecurity strategies compare to global best practices [13], [14].
   - Gap: Lack of cross-country comparative studies to benchmark Bangladesh's fintech and cybersecurity landscape against similar economies.
6. Limited Empirical Studies on AI, Blockchain, and Fintech Security Innovations
   - Rahman discusses blockchain and AI in fintech, but there is limited empirical data on their effectiveness in improving banking cybersecurity. Few studies assess how AI-driven fraud detection and blockchain-based security solutions are being implemented in Bangladesh's financial institutions.
   - Gap: Need for empirical research on AI and blockchain applications in securing fintech transactions.

2. Materials and Methods

The research methodology outlines the design, data collection methods, analytical techniques, and ethical considerations used to explore the fintech landscape and cybersecurity challenges in banking operations in Bangladesh. The methodology ensures a systematic, reliable, and valid approach to answer the research questions.

A. Research Design

This study adopts a mixed-methods approach, combining quantitative and qualitative research methods to provide a comprehensive analysis of fintech adoption and cybersecurity in banking operations.

A-1: Quantitative Approach

Used to analyze the impact of fintech adoption on banking efficiency and cybersecurity risks. Includes surveys and statistical analysis to measure factors such as consumer adoption, cybersecurity threats, and regulatory compliance levels

A-2: Qualitative Approach

Used to explore expert opinions, industry trends, and regulatory challenges. Includes interviews and case studies with banking professionals, fintech developers, and cybersecurity experts.

B. Data Collection Methods

B-1: Primary Data Collection

Primary data is gathered through:

- Surveys & Questionnaires
- Interviews with Industry Experts
- Case Studies of Bangladeshi Banks & Fintech Firms

B-2: Secondary Data Collection

- Bangladesh Bank reports on fintech policies, cybersecurity regulations, and financial inclusion.
- Academic journal articles on cyber threats, fintech growth, and digital banking security.
- Global reports from World Bank, IMF, and BIS on fintech and cybersecurity trends.

C. Data Analysis Techniques

C-1: Quantitative Data Analysis

- Descriptive Statistics: Mean, standard deviation, and frequency distribution to analyze fintech adoption trends.
- Regression Analysis: To test hypotheses on the relationship between fintech adoption and cybersecurity risks.
- Chi-Square Test: To examine the association between customer trust and fintech adoption.

C-2: Qualitative Data Analysis

- Thematic Analysis: Used for expert interviews to identify key themes in cybersecurity policies, fintech integration, and regulatory gaps.
- Content Analysis: Applied to case studies and regulatory reports to evaluate cybersecurity threats and fintech policy effectiveness.

D. Sampling Strategy

- Target Population: Banking customers, fintech users, banking professionals, cybersecurity experts, and policymakers in Bangladesh.
- Sample Size:
  - Surveys: 315 respondents (ensuring statistical significance).
  - Interviews: Around 35 industry experts (to gather in-depth insights).

E. Sampling Technique

- Stratified Random Sampling for surveys ensuring representation across different customer segments and banks.
- Purposive Sampling for expert interviews selecting participants with expertise in fintech and cybersecurity.

F. Ethical Considerations

Participants will be informed about the purpose, risks, and confidentiality of the study. Survey responses and interview data will be anonymized to protect participant identities. The research will comply with Bangladesh Bank's data protection guidelines and global ethical research standards.

G. Research Limitations

- Self-Reported Data Bias
- Limited Access to Cybersecurity Data
- Rapid Technological Changes

H. Justification of Research Methodology

The methodology aligns with global best practices in fintech research and cybersecurity risk assessment.

- The mixed-methods approach ensures a holistic analysis, combining statistical rigor with expert insights.
- Quantitative analysis: provides empirical evidence on fintech adoption and cybersecurity risks.
- Qualitative analysis: captures contextual insights from industry professionals**.**

I. Research Questions:

In this research the questionnaires for supplementary research.

- Central research questions: What is the current situation of the Fintech Landscape & Cybersecurity of the Banking Operations in Bangladesh?
- Supplementary research questions: What are the outcomes of the PESTLE analyses of Fintech Landscape & Cybersecurity of the Banking Operations in Bangladesh? And What changes are required to foster the growth of this sector?

SIGNIFICANCE AND IMPLICATIONS OF THE RESEARCH

This study bridges the gap between fintech adoption and cybersecurity risk management, which has not been extensively explored in the Bangladeshi context. It integrates technology acceptance models with cybersecurity risk frameworks, providing a holistic view of fintech adoption and security challenges [15]. Most existing research focuses on developed economies, leaving a research gap in fintech-driven banking security in developing economies like Bangladesh. This study contributes to South Asian fintech security research, offering a model applicable to other emerging fintech markets [16].

The findings highlight key cybersecurity threats (phishing, ransomware, data breaches) in digital banking and recommend proactive security measures. Helps financial institutions adopt stronger authentication, encryption, AI-driven fraud detection, and blockchain security [17]. Banks and fintech firms can use the findings to develop customer-centric digital financial services with enhanced security features. Insights on consumer trust in fintech security help firms improve mobile banking, digital wallets, and online payment systems [18].Provides empirical evidence on the effectiveness of Bangladesh Bank's ICT Security Guidelines [19]. Helps policymakers design data protection laws, fintech licensing policies, and cross-border cybersecurity collaborations .The study explores how secure fintech solutions can expand financial access to unbanked and rural populations. Encourages banks to invest in secure mobile financial services (MFS) like bKash, Nagad, and Rocket [20].Encourages future studies on AI-powered fraud detection, blockchain-based security in banking, and biometric authentication [21].

3. Results

Questionnaires survey and interviews were arranged among 315 participants including industry experts in the target and different segment. The most average outcome and ratio are analyzed as applicable. The outcome of primary and secondary are illustrated as applicable.

1. Beneficiaries and Stakeholders Perspective:

Customers face increasing risks of cyber fraud, phishing, and data breaches due to weak security frameworks. Many customers, particularly in rural areas, lack awareness of fintech services and cybersecurity measures. Fintech firms and banks struggle with unclear regulatory frameworks, making compliance challenging. Many banks use outdated security systems, increasing vulnerability to cyberattacks. Different fintech platforms lack integration, causing inefficiencies in transactions. Banks and fintech firms face complex compliance requirements that slow innovation. High costs of cybersecurity infrastructure deter many financial institutions from upgrading their security. Many users perceive fintech as a risky option due to cyber threats. Urban customers are more willing to adopt digital banking, while rural users remain skeptical. Trust in traditional banking remains higher than in fintech solutions.

2. Financial Intermediaries:

Financial intermediaries are prime targets for cybercriminals, leading to data breaches, ransomware attacks, and financial fraud. These risks are exacerbated due to insufficient investment in cybersecurity infrastructure. With the rise of digital transactions, fraud poses a significant challenge for financial intermediaries. Financial intermediaries often face regulatory challenges because of unclear and evolving guidelines from regulators. The absence of clear cybersecurity and data protection laws adds complexity. This leads to system vulnerabilities and compromises in data security. This puts pressure on traditional financial institutions to adopt digital solutions or risk losing customers.

International fintech players also pose competition in the local market, creating challenges for local financial intermediaries to stay competitive and secure their customer base. However, many are starting to view fintech as a necessary partner to expand their services and improve efficiency. Financial intermediaries often feel that the regulatory framework in Bangladesh is not flexible enough to encourage innovation while maintaining financial stability. This results in frustration and operational delays. There is widespread public concern about the stability of fintech firms and the potential for these entities to fail, leaving customers without recourse to recover their funds. Customers often perceive digital banking and fintech services as less secure than traditional banking services. There is a strong belief that physical branches offer a sense of security that digital-only services cannot provide.

3. Service Delivered Perspectives:

Financial institutions face a significant risk of data theft and privacy violations due to inadequate security protocols and increasing cyber threats. This compromises customers' financial and personal data. Increased use of mobile banking and online payment systems exposes users to the risk of fraud, identity theft, and unauthorized transactions [22]. Banks and fintech services often experience technical issues, including system outages or downtime during peak periods, disrupting service delivery and damaging consumer trust. Inadequate infrastructure in rural and remote areas limits access to digital banking services, creating a gap in service delivery between urban and rural areas. Due to constantly evolving fintech and cybersecurity regulations, service providers may inadvertently fail to comply with the legal requirements, leading to penalties, legal issues, and loss of consumer confidence. Regulators may not act swiftly to address new challenges, such as the introduction of disruptive fintech models leading to regulatory gaps.

Many customers, especially older generations or those in rural areas, lack the digital literacy needed to use fintech services effectively, leading to low adoption rates. Fintech services are perceived as too complex for many users, with the registration process or use of digital wallets, for instance, being seen as challenging and unfamiliar. Service interruptions in digital banking, especially with mobile financial services, hinder customer experience, trust, and the overall delivery of financial services. The quality of customer service provided by digital platforms and traditional banks is inconsistent,

with many customers facing issues such as delayed transactions or poor user interfaces. There is a general reluctance among certain customer segments to embrace fintech services due to security concerns and the fear of fraud or money loss. Banks and fintech firms often face the challenge of balancing cost-efficiency with high service quality. Investments in secure infrastructure and cutting-edge technology are expensive and can be a barrier to scaling services

4. Regulatory Framework:

   Fintech and cybersecurity regulations are still evolving, leading to uncertainty among banks and fintech firms. This uncertainty makes it difficult for institutions to plan long-term investments and innovations confidently. The lack of clear, specific rules for emerging technologies like as blockchain, AI-driven financial services create ambiguity, forcing institutions to interpret general financial regulations in a digital context. Several agencies have roles in governing fintech and cybersecurity. This can lead to overlapping jurisdictions and inconsistencies in policy enforcement. Regulatory bodies often lack the resources and technical expertise needed to enforce complex cybersecurity and fintech regulations effectively. This can result in inconsistent enforcement and compliance lapses.

   The rapid pace of fintech innovation often outstrips the regulatory framework, which struggles to update policies in a timely manner. Regulations designed for traditional banking systems may not be effective in mitigating risks associated with new digital platforms, leaving gaps in cybersecurity protections. Existing cybersecurity regulations may not comprehensively address the unique threats posed by digital financial services, such as data breaches, ransomware, and phishing attacks. Enhanced collaboration could lead to more balanced regulations that protect consumers while fostering innovation and competitiveness within the fintech sector. Many in the fintech community feel that the regulatory environment is overly cautious, potentially stifling innovation with excessive compliance demands.

5. Global Operations and Analytical views:

   Financial institutions in Bangladesh face risks from international cybercriminals, such as ransomware, phishing, and identity theft. Attacks like the 2016 Bangladesh Bank heist highlight vulnerabilities in cross-border transactions . International financial regulations impose stringent cybersecurity and data privacy requirements, creating compliance challenges for Bangladeshi banks. Many banks in Bangladesh still rely on outdated core banking systems, making global fintech integration slow and costly . International remittances and cross-border payments often face high transaction fees, delays, and complex compliance processes .

   Regulations in Bangladesh often lag behind global best practices, limiting fintech growth and investor confidence. Bangladesh lacks skilled professionals trained in AI-driven fraud detection, ethical hacking, and blockchain security, hindering global fintech competitiveness. Many financial professionals lack deep expertise in fintech risk assessment and regulatory compliance, slowing global fintech adoption Despite a growing fintech sector, Bangladesh has yet to attract significant FDI from global fintech giants like Stripe, Revolt, or Square. Only 40% of banks in Bangladesh have a dedicated cybersecurity operations center (SOC), far lower than global standards (Deloitte Global Risk Report, 2023 Services like bKash, Nagad, and Rocket process over $90 billion annually, yet global players like PayPal and Stripe remain absent from the market . Global investors remain cautious due to bureaucratic red tape, complex licensing requirements, and inconsistent fintech regulations. Bangladesh has faced money laundering concerns, affecting its global reputation for fintech and banking transparency. While fintech adoption is rising, 40% of Bangladeshis still prefer cash transactions, citing cybersecurity concerns. Many customers fear fraud, hidden charges, and data misuse from unregulated fintech lenders.

4. Discussion

A. Limitations

This section outlines the limitations of the study, followed by the key findings, and provides an in-depth discussion based on the analysis of fintech adoption and cybersecurity challenges within the banking sector in Bangladesh. The findings and discussions are tied to existing literature, offering a holistic view of the research. While the study aimed for a comprehensive understanding, the survey sample was limited to a few banks and fintech firms due to time and resource constraints. This may not fully represent the broader diversity of banks (e.g., private, public, and foreign banks) and fintech startups operating across Bangladesh . The study primarily used surveys and interviews for primary data collection. As with many self-reported data methods, there is a risk of response bias, where participants may provide socially desirable answers rather than objective responses, particularly regarding their bank's cybersecurity practices or fintech usage

Banking institutions were hesitant to disclose sensitive cybersecurity incidents or breaches due to confidentiality and security concerns. This limited the study's ability to analyze real-world cyberattack case studies and their impact on customer trust or bank performance. The technological landscape of fintech and cybersecurity threats is fast-evolving. As such, the findings of this study may become outdated as new threats, regulations, and technologies emerge. The dynamic nature of fintech innovation presents challenges in ensuring the timeliness and relevance of research findings.

B. Findings

A significant portion of the population in Bangladesh has adopted mobile financial services (MFS), such as bKash, Rocket, and Rocket, demonstrating substantial progress in financial inclusion. Customers are increasingly adopting mobile banking and digital wallets for day-to-day transactions, particularly in rural areas. However, cybersecurity concerns remain a barrier to adoption, with customers seeking more secure digital platforms . The banking sector is experiencing an uptick in cybersecurity incidents, such as phishing attacks, ransomware, and data breaches. The study identifies these as primary concerns for both customers and financial institutions. Despite technological advancements, many banks continue to face significant security gaps in their digital platforms. Issues such as weak encryption, lack of multi-factor authentication (MFA), and limited employee training on cybersecurity were highlighted While the Bangladesh Bank's ICT Security Guidelines have set standards for cybersecurity practices, there is a lack of uniformity in implementation across banks and fintech firms. Several institutions face challenges in compliance due to the lack of adequate resources and knowledge of evolving cybersecurity standards. Moreover, cross-border regulatory issues complicate the protection of financial data in a globalized fintech . Despite the growing use of fintech, many consumers remain wary of digital financial services due to concerns over data privacy and cybersecurity. Trust remains a critical factor that influences fintech adoption, and banks must work towards building consumer confidence through transparent security practices.

C. Discussions

The rapid rise of fintech in Bangladesh has contributed significantly to financial inclusion, enabling millions of previously unbanked individuals to access essential financial services. Services like mobile wallets, micro-lending, and remittances have bridged the financial gap in rural and underserved areas. However, this growth needs to be balanced with robust cybersecurity practices to mitigate the risks of financial fraud and identity theft. Banks should prioritize integrating

secure and user-friendly fintech solutions to increase adoption while ensuring data privacy and security for customers. Enhanced digital literacy initiatives can further boost consumer confidence and trust .

The study identifies significant gaps in cybersecurity practices within Bangladesh's banking sector, particularly in digital banking channels. The absence of advanced encryption, multi-factor authentication, and regular system audits leaves financial institutions vulnerable to cyberattacks. The findings suggest that while cybersecurity is becoming a top priority, many institutions are still lagging in implementing effective solutions. To tackle these challenges, banks and fintech firms should adopt AI-powered fraud detection systems, end-to-end encryption, and blockchain technology for secure transactions. Moreover, employee training and awareness programs must be implemented to prevent human errors that often lead to security breaches . While Bangladesh Bank has issued guidelines to protect ICT infrastructure in the financial sector, the research reveals that regulatory enforcement remains weak across smaller banks and fintech startups. Furthermore, cross-border cybersecurity laws are underdeveloped, exposing banks to risks from international cyber threats. Policymakers must improve the enforcement of existing regulations and ensure that financial institutions comply with the highest security standards. There is a need for collaboration between regulators, banks, and fintech companies to enhance the national cybersecurity framework and cross-border data protection .Consumer Awareness: The findings highlight the need for consumer education in understanding cybersecurity risks and the importance of using secure digital banking services. Cybersecurity awareness campaigns can play a pivotal role in building trust in fintech services. Financial institutions should adopt transparent security practices and communicate them clearly to consumers. Offering features such as fraud protection services, instant account alerts, and 24/7 customer support can enhance consumer trust and encourage wider adoption of digital financial services.

5. Conclusion

This study provides a comprehensive analysis of the fintech landscape and cybersecurity challenges within the banking sector of Bangladesh, focusing on the increasing role of digital financial services and the accompanying cybersecurity risks. It underscores the transformational potential of fintech in driving financial inclusion, enhancing digital banking experiences, and supporting the overall economic growth of the nation. However, it also highlights several critical cybersecurity concerns that need urgent attention to safeguard the integrity of digital transactions and protect consumers' sensitive financial data. This research sheds light on the dual forces shaping Bangladesh's banking landscape are the expansion of fintech and the growing cybersecurity risks that accompany digital financial services. The country's journey towards a digitally inclusive financial ecosystem hinges on addressing security challenges and fostering consumer trust in fintech solutions. By strengthening the regulatory framework, improving security measures, and promoting consumer education, Bangladesh can unlock the full potential of its fintech sector, ensuring a secure, resilient, and inclusive banking environment for the future.

REFERENCES

[1]. T. Ahmed and R. Hossain, "Cybersecurity Threats in Bangladesh's Banking Sector: A Critical Analysis," Journal of Financial Security, vol. 12, no. 4, pp. 55–72, 2020.
[2]. Asian Development Bank (ADB), Digital Skills Report, 2023. Accessed: Jan. 31, 2025.
[3]. Bangladesh Bank, Guidelines on ICT Security for Banks and Financial Institutions, 2023.

[4]. BASIS, Fintech Report and Bangladesh Fintech Consumer Trust Index, 2023.
[5]. Bangladesh Telecommunication Regulatory Commission (BTRC), BTRC Report, 2023. Accessed: Jan. 31, 2025.
[6]. Bangladesh Cyber Security Index (BCSI), Cybercrime Threat Intelligence Report, 2023.
[7]. Bangladesh Ministry of Finance, Bangladesh Economic Review, 2023. Accessed: Jan. 31, 2025.
[8]. Bangladesh Fintech Association, 2023. Accessed: Jan. 29, 2025.
[9]. Bangladesh Fintech Policy Report, 2023. Accessed: Feb. 20, 2025.
[10]. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, SAGE Publications, 2014.
[11]. A. Field, Discovering Statistics Using IBM SPSS Statistics, SAGE Publications, 2018.
[12]. M. Hasan, S. Karim, and T. Alam, "Cyber Threats and Banking Security in Bangladesh: Strategies for Risk Mitigation," International Journal of Financial Technology, vol. 18, no. 2, pp. 89–102, 2021.
[13]. IMF, Fintech Regulations Report, 2023. Accessed: Feb. 28, 2025.
[14]. N. Islam, S. Rahman, and M. Jahan, "Emerging Technologies in Fintech: Implications for Banking in Bangladesh," Journal of Digital Finance, vol. 9, no. 1, pp. 27–45, 2021.
[15]. R. Karim and S. Alam, "Fintech Adoption in Bangladesh: Opportunities and Challenges," International Journal of Fintech Studies, vol. 10, no. 2, pp. 112–130, 2020.
[16]. R. Khan and M. Rahman, "Regulatory Challenges in Cybersecurity for Bangladesh's Financial Institutions," Financial Policy Review, vol. 15, no. 3, pp. 110–129, 2022.
[17]. McKinsey & Company, Fintech Report and Asia Digital Banking Survey, 2023.
[18]. Rahman and M. Alam, "The Impact of Mobile Financial Services on Banking in Bangladesh: A Fintech Perspective," South Asian Journal of Economic Studies, vol. 14, no. 2, pp. 120–140, 2022.
[19]. M. S. Rahman, "Cybersecurity in Banking: A Case Study of Bangladesh," Journal of Financial Technology, vol. 15, no. 3, pp. 45–60, 2021.
[20]. SWIFT, Security Report, 2023. Accessed: Mar. 2, 2025.
[21]. World Bank, Digital Financial Services in South Asia: Trends and Challenges, 2022.
[22]. World Bank, World Bank Digital Finance Report, 2023.