Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(11), 223-235
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

AI-Driven Cybersecurity Challenges in Bangladesh's Banking Industry

Aslam Khan[1], Bikash Kumar Saha Roy[2], Aktaruzzaman Sarker[2], Syed Noman Abedin[2], Md. Mominul Islam[2], Moinul Zaber[2]

[1]Colangelo College of Business, Grand Canyon University, Phoenix, Arizona, USA
[2]Department of Computer Science and Engineering, World University of Bangladesh, Dhaka, Bangladesh
Email: mail2aslkh@gmail.com, talk2rajucis@gmail.com, sarkerma@gmail.com, syednomanabedin@gmail.com, itmominul@gmail.com, zaber@du.ac.bd

How to cite this paper: Khan, A., Roy, B.K.S., Sarker, A., Abedin, S.N., Islam, Md.M. and Zaber, M. (2025) AI-Driven Cybersecurity Challenges in Bangladesh's Banking Industry. *Journal of Computer and Communications*, **13**, 223-235.
https://doi.org/10.4236/jcc.2025.1311014

Received: September 24, 2025
Accepted: November 24, 2025
Published: November 27, 2025

Abstract

This report delves into the key challenges and opportunities that banks in Bangladesh face in adopting AI-powered cybersecurity measures. It highlights several critical issues, such as a lack of skilled cybersecurity personnel, insufficient employee training, limited use of AI in banking operations, and obstacles to AI adoption. These problems prevent banks from fully harnessing the potential of AI to tackle the growing complexity of cyber threats. To address these challenges, the report offers practical recommendations, including expanding cybersecurity teams with AI expertise, improving training programs for employees, broadening AI applications across various banking functions, optimizing existing AI systems, and adopting AI-specific compliance frameworks. The report also underscores the need for collaboration between banks, regulators, and tech providers to enhance regulatory support and access to advanced AI tools. Ultimately, it stresses the urgency for Bangladesh's banking sector to address AI-driven cybersecurity threats and implement best practices to protect sensitive information, improve efficiency, and build resilience against evolving cyber risks.

Keywords

AI-Powered Cybersecurity, Banking Sector, Cybersecurity Personnel, AI Adoption, Regulatory Support

1. Introduction

Artificial intelligence (AI) is reshaping industries worldwide, driving unprecedented levels of efficiency and innovation. Businesses are increasingly leveraging

AI to streamline operations, enhance customer experiences, and unlock new opportunities [1]. However, this technological revolution also has a darker side: cybercriminals are harnessing AI to develop more sophisticated and harder-to-detect attack methods. From AI-powered malware that adapts to evade detection to deepfake scams that manipulate voices and images with alarming accuracy, the threat landscape is evolving rapidly [2]. Phishing attacks have become more convincing, while vulnerabilities in Internet of Things (IoT) devices are being exploited with increasing precision [3]. These advancements in cybercrime are not just theoretical; they are real, growing, and increasingly dangerous.

For Bangladesh, these developments are particularly concerning, especially in the banking sector, which is undergoing rapid digital transformation. While the adoption of digital services has brought convenience and accessibility to millions, it has also exposed critical weaknesses. Many banks still rely on outdated systems and lack robust security infrastructure, making them vulnerable to cyberattacks [4]. Compounding the problem is a severe shortage of skilled cybersecurity professionals who can defend against advanced threats. The 2016 Bangladesh Bank heist, in which hackers stole USD 81 million by exploiting vulnerabilities in the bank's systems, serves as a stark reminder of these risks [5]. Yet, years later, many financial institutions in the country remain underprepared to face today's sophisticated cyber threats.

To navigate this challenging landscape, Bangladesh's banking sector must take decisive action. Upgrading outdated systems and investing in modern cybersecurity technologies is no longer optional; it is a necessity. Equally important is cultivating a pool of cybersecurity talent through training programs, partnerships with educational institutions, and attracting global experts. Stricter regulations must also be enforced to ensure that banks adhere to the highest security standards [6]. However, technology and regulations alone are not enough. Human factors play a critical role in cybersecurity, which is why banks must prioritize educating both employees and customers about digital security best practices [7]. From recognizing phishing attempts to safeguarding personal information, awareness can be a powerful defense.

2. Present Scenario

Bangladesh's banking sector plays a vital role in driving the country's economic growth by supporting businesses, enabling financial inclusion, and serving millions of customers. In recent years, it has embraced rapid digital transformation, with mobile apps, online banking, and automated systems reshaping how people manage their finances. While these advancements offer speed and convenience, they have also exposed the sector to growing cybersecurity threats [4].

As banks rely more on digital platforms, they become prime targets for cybercriminals due to the vast amount of sensitive financial data they manage. A defining example was the 2016 Bangladesh Bank heist, when hackers stole USD 81 million by exploiting system weaknesses [5]. Such incidents highlight not only tech-

nical gaps but also how cyberattacks can erode public trust, a key pillar of digital banking. Today, threats like phishing, ransomware, and data breaches are becoming more frequent and sophisticated [3].

Although regulations exist to protect the sector, many banks still face challenges such as outdated systems, weak security measures, and a shortage of cybersecurity experts [6]. These vulnerabilities make them ill-prepared for modern cyber risks. Strengthening cybersecurity is therefore not just a technical task; it is essential for safeguarding data, ensuring financial stability, and maintaining public trust [7].

This study explores the key cybersecurity challenges in Bangladesh's banking sector, the factors that make it vulnerable, and their potential consequences. It also outlines practical solutions, including modernizing infrastructure, investing in advanced security technologies, and developing skilled cybersecurity talent through training and education. By taking a proactive and collaborative approach, the banking sector can create a safer digital environment that supports economic growth and builds customer confidence [1].

3. Background

AI has become a powerful yet complex force in cybersecurity. It helps defenders detect and respond to threats faster and more accurately through machine learning and automation, spotting suspicious patterns and neutralizing attacks in real time [1]. At the same time, cybercriminals are exploiting AI to create more advanced, targeted, and difficult-to-detect attacks. Deepfake scams, AI-driven phishing, and adaptive malware highlight how AI can be used to outsmart traditional defenses [2] [3].

This escalating battle between attackers and defenders poses serious risks for rapidly digitalizing countries like Bangladesh. While digital services have boosted connectivity and economic growth, they have also exposed critical security gaps. To strengthen defenses, the country introduced its National Cybersecurity Strategy in 2014, building a legal and collaborative framework for a safer digital ecosystem [6]. Progress has been made, but significant challenges persist.

Many sectors, especially banking, healthcare, and government, still rely on outdated systems, making them vulnerable to modern attacks. Compounding this problem is a shortage of skilled cybersecurity professionals and uneven public awareness [4]. In 2022 alone, more than 63,000 cybercrime incidents were reported, reflecting the scale of the issue.

Closing this gap requires investment in people, technology, and awareness. Expanding cybersecurity education, launching nationwide awareness campaigns, and deploying AI-based security solutions are essential steps. With Bangladesh's cybersecurity market expected to grow to USD 368.8 million by 2029, the country has both a challenge and an opportunity to build resilience [7].

By modernizing infrastructure, developing talent, and fostering a culture of cybersecurity, Bangladesh can better protect its digital transformation. Though the

threats are evolving, a proactive and united approach can secure the nation's digital future.

4. Methodology

To collect reliable insights for this study, a mixed qualitative approach was used, combining in-depth interviews with semi-structured questionnaires. Using purposive sampling, 40 participants, both IT and non-IT professionals from private and government banks, were selected to capture diverse perspectives on cybersecurity in Bangladesh's banking sector [8].

The research covered institutions of different sizes and regions to reflect the broader banking landscape. Data collection spanned October to December 2024, allowing sufficient time for engagement and observation. Interviews provided rich qualitative narratives, revealing challenges such as outdated infrastructure, limited cybersecurity skills, and low awareness levels. Questionnaires ensured structured and comparable data across respondents, reinforcing interview findings [9].

This human-centered approach offered a holistic view of the sector's cybersecurity landscape, emphasizing the urgency for modernization, capacity building, and stronger regulatory frameworks. By integrating multiple data sources, the study provides practical, context-specific recommendations for improving cybersecurity resilience in Bangladesh's financial institutions [10].

5. Result

A targeted survey was carried out to examine the impact of AI-driven cybersecurity threats on Bangladesh's banking sector. It involved 33 participants from seven major banks, including IT professionals, cybersecurity specialists, and senior banking officials. This diverse group provided a balanced perspective on technical vulnerabilities, evolving threat patterns, and organizational readiness. The survey focused on identifying AI-enhanced threats such as phishing, adaptive malware, and fraudulent transactions; evaluating banks' preparedness and adoption of AI defenses; and exploring practical solutions like technology upgrades, increased investments, and stronger collaboration [2] [3].

The results highlighted significant gaps in awareness and preparedness. Only 52% of respondents demonstrated strong knowledge of AI-enabled threats, and just 40% of banks had adopted AI-powered detection tools. Larger institutions were more advanced in adopting AI defenses, while smaller banks lagged behind due to limited resources, leaving the sector unevenly protected. Regulatory frameworks also lacked clarity, and limited industry collaboration further weakened collective defense efforts [7].

To address these challenges, the study suggests a multi-layered approach: expanding AI-focused employee training, investing in real-time monitoring technologies, and encouraging banks to share threat intelligence and best practices. While AI offers powerful tools for detection and fraud prevention, issues like high costs, integration challenges, skills shortages, and ethical concerns must be ad-

dressed to ensure robust security [10]. A more collaborative, well-resourced ecosystem can help protect Bangladesh's banking infrastructure and build long-term resilience.

6. Discussion

The survey results reveal several pressing gaps that must be addressed to strengthen the banking sector's adoption of AI-driven cybersecurity solutions. One of the most critical issues is the shortage of skilled cybersecurity professionals. Around 70% of banks have fewer than 50 employees dedicated to cybersecurity, resulting in overworked and understaffed teams [11]. This finding underscores the urgent need to invest in workforce development, including partnerships with universities and training institutions to build a sustainable talent pipeline.

Although many employees are aware of AI-related threats, only a small proportion feel adequately prepared to respond to them. This reflects a gap between awareness and practical capability, which could be bridged through structured, hands-on training programs and continuous professional development [12].

Currently, AI tools are mainly deployed for fraud detection and risk management, but their potential remains underutilized in areas such as customer service automation and credit risk assessment. Furthermore, there is a perception that existing AI systems are not fully optimized, particularly when addressing operational inefficiencies, signaling the need for better integration and system refinement [13].

The reliance on outsourcing IT infrastructure adds another layer of risk, particularly concerning data security and vendor accountability. This highlights the importance of robust contractual safeguards and independent security audits to protect sensitive financial data [2].

Other key barriers to AI adoption include limited financial resources, a lack of skilled personnel, and ambiguous regulatory frameworks. Moreover, many employees are not actively engaged in AI implementation processes, indicating the need for broader organizational education and participation to foster a security-aware culture [7] [14].

Finally, adopting structured AI-specific compliance frameworks, such as the NIST AI Risk Management Framework, can support organizations in managing AI-related risks more effectively and responsibly [15].

7. Challenges and Global Comparison

The survey reveals several barriers to effective AI-driven cybersecurity in the banking sector:

1. Cybersecurity Skills Gap: Around 70% of banks employ fewer than 50 cybersecurity staff, mirroring a global talent shortage and the need for targeted recruitment and training [16].

2. Low Confidence in AI Risk Response: Although 60% of employees are aware of AI threats, only 9.1% feel equipped to handle them. Globally, experts stress scenario-based training to boost confidence and skills [17] [18].

3. Limited AI Applications: AI use remains focused on fraud detection, while other areas like customer service and credit scoring are underutilized. Internationally, banks are expanding AI into broader operational domains [19] [20].

4. Effectiveness Gaps: Only 25% of respondents view AI as highly effective, pointing to optimization needs. Continuous monitoring and iterative improvements are key global practices [21].

5. Adoption Barriers: A lack of skilled staff (56.3%) and financial constraints (9.4%) slow AI adoption. A phased approach supported by regulatory clarity is recommended [22].

6. Weak AI Compliance: Few banks follow structured frameworks like the NIST AI RMF. Global institutions urge wider adoption for stronger governance [23].

7. Regulatory & Technological Gaps: Unclear regulations (46.7%) and limited tools (56.7%) remain major obstacles. Clearer rules and better technology are global priorities [20].

8. Training Priority: A strong majority (73.3%) identify workforce training as essential. This aligns with the global consensus on building AI security skills through structured education [16].

8. Analysis

The respondents include professionals from the banking and IT sectors, with the following breakdown: IT security specialists (21.2%), cybersecurity analysts (18.2%), risk management professionals (27.3%), AI specialists (6.1%), and other professionals (39.4%) (Figure 1).

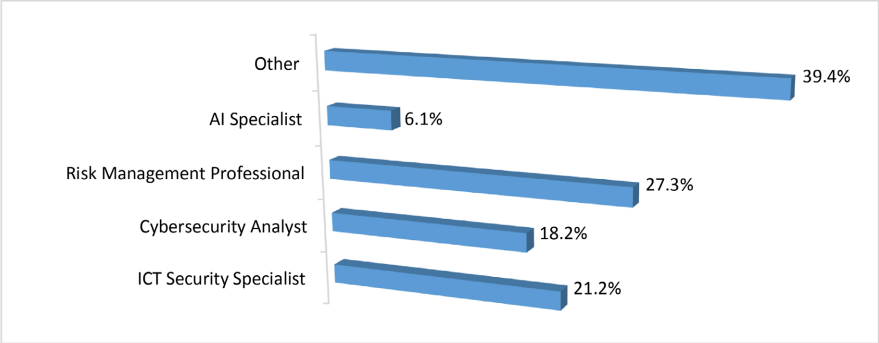

Figure 1. Responded role in cybersecurity.

Figure 2 shows the distribution of cybersecurity personnel working in selected banks was identified as follows: 69.7% of banks have between 1 - 50 employees, 12.1% have 51 - 100 employees, 9.1% have 101 - 500 employees, and 9.1% have more than 500 employees.

More than 60% of employees are aware of the increasing AI-based cybersecurity risks in the banking sector, whereas the ability to eliminate these risks is relatively low, at 9.1%. However, 30.3% of respondents believe that AI-driven threats are less significant than human-based threats (Figure 3).

Various AI applications are used in the banking sector to detect, identify, and protect data from hackers. In Bangladesh, the following AI tools are utilized: 41.4% for fraud detection, 20.7% for credit scoring, 37.9% for customer service automation, 48.3% for risk management, and 20.7% for other purposes (Figure 4).

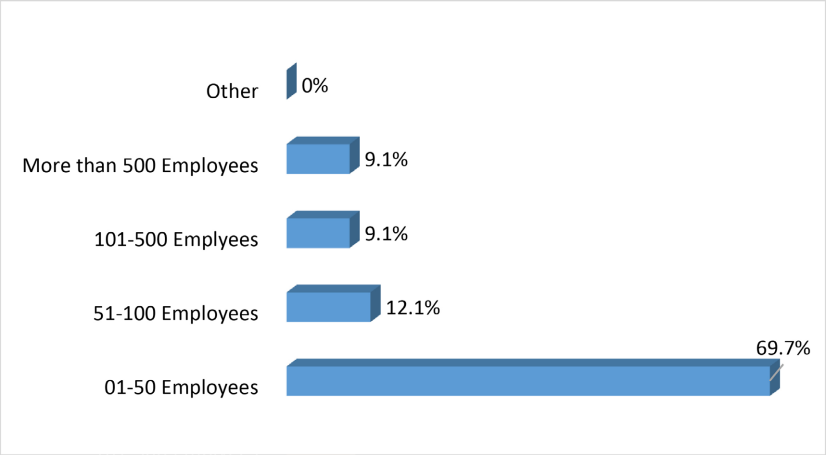

Figure 2. The number of cybersecurity personnel working in banks.

Figure 3. Perception of AI-Dirven common threat.

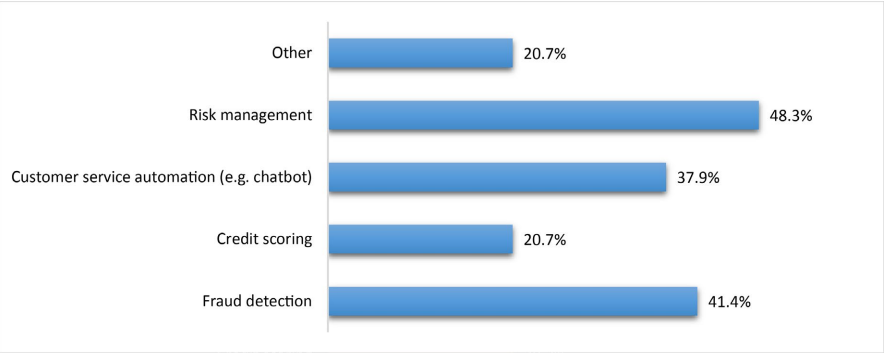

Figure 4. AI application used in the Banking sector presently.

Data analysis shows that 59.4% of respondents view AI as effective in tackling

operational challenges, while 25% find it highly effective and 15.6% rate it as moderately effective (Figure 5). This reflects a generally positive perception of AI's role in boosting operational efficiency.

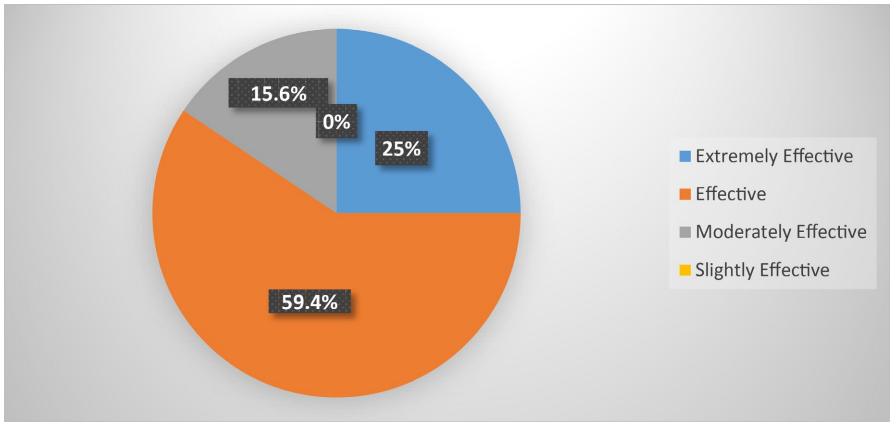

Figure 5. Effectiveness of AI in overcoming operational challenges at the banking sector in Bangladesh.

Survey results indicate that 35.5% of respondents see AI reducing costs, another 35.5% cite improved operational efficiency, 16.1% value access to specialized expertise, and 12.9% highlight better focus on core business functions (Figure 6). Overall, AI adoption offers cost savings, efficiency gains, and enhanced strategic focus.

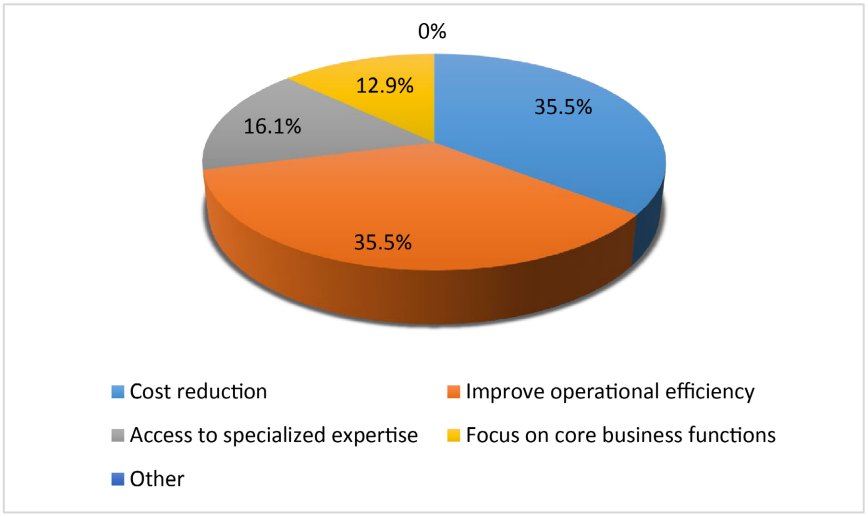

Figure 6. Benefits of IT assets outsourcing.

Banks in Bangladesh face several challenges with IT asset outsourcing. 40.6% of respondents cited data security and confidentiality risks, 28.1% noted service quality issues, 18.8% highlighted compliance challenges, and 12.5% pointed to limited control over assets (Figure 7). These findings emphasize the need for robust management frameworks to ensure security, performance, compliance, and oversight in outsourcing.

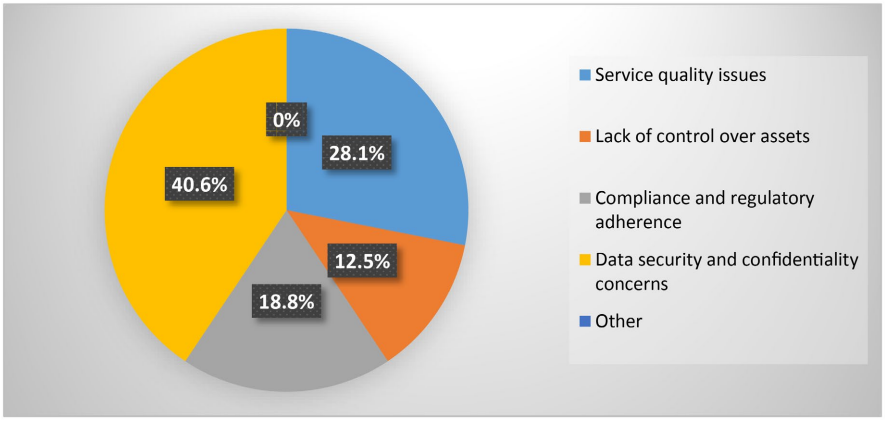

Figure 7. Key challenges of IT assets outsourcing management.

Implementing AI-driven cybersecurity in banks faces key challenges: 56.3% cite a shortage of skilled personnel, 9.4% note financial constraints, 15.6% highlight unclear regulations, and 12.5% point to rapidly evolving AI threats (**Figure 8**). Addressing these requires training, funding, regulatory clarity, and proactive threat management.

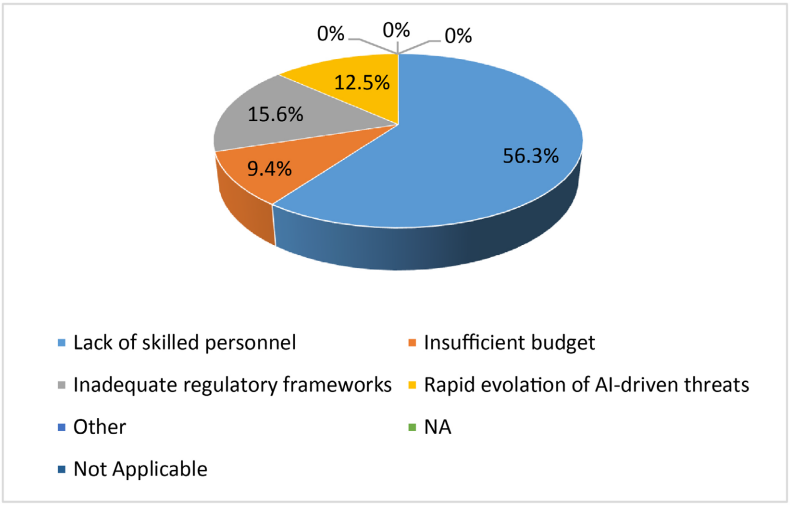

Figure 8. Challenges to implement AI cybersecurity measures.

The survey shows that 45.5% of banking staff are directly involved in AI implementation, contributing to system design, deployment, and management. However, 54.5% are not engaged, often due to limited skills or non-technical roles (**Figure 9**). This gap highlights the need for training, awareness programs, and strategies to involve more employees in AI initiatives.

The survey shows varied adoption of cybersecurity frameworks in banks. 56.7% use ISO/IEC 27001 and 42001, 16.7% follow the NIST AI Risk Management Framework, 23.3% comply with GDPR, SOC, or HIPAA, and 33.3% use the SWIFT Customer Security Programme. Most banks (83.3%) adhere to Bangladesh Bank Guidelines V4.0 (**Figure 10**). While global and local standards are widely used,

AI-specific risk strategies remain underutilized.

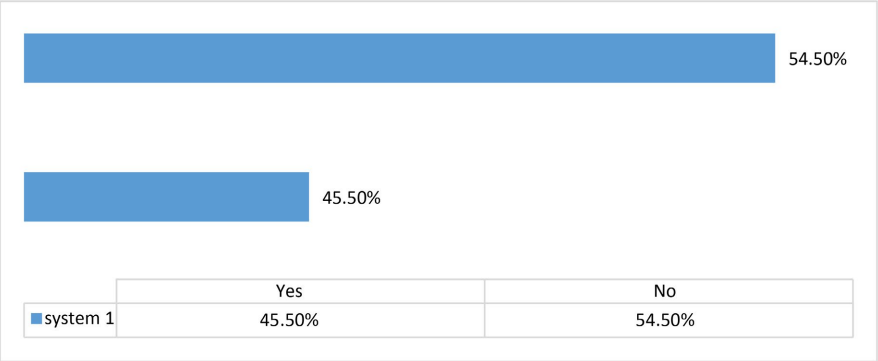

Figure 9. Direct involvement in an AI system.

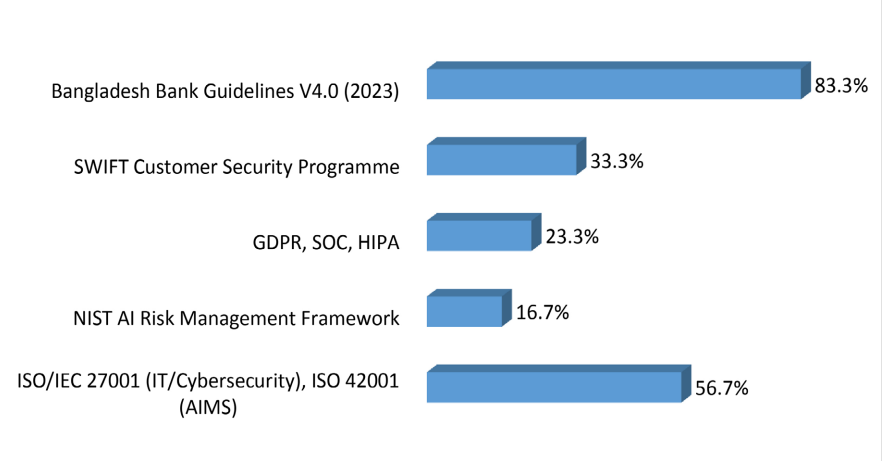

Figure 10. Applicable national & international standards in the banking sector presently.

To enhance cybersecurity and resilience in Bangladesh's banking sector, key measures include stronger regulatory support (46.7%), the adoption of advanced AI-powered tools (56.7%), increased investment in workforce training and skill development (73.3%), and fostering industry-wide collaboration (36.7%) to address evolving threats and drive innovation (Figure 11).

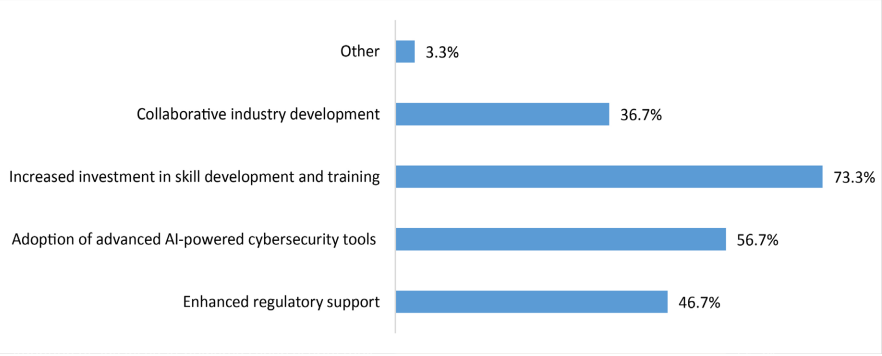

Figure 11. Additional measures recommended for AI security improvement.

As AI-driven threats continue to rise in the banking sector, staff members are calling for swift action in several key areas to address these challenges. The most pressing concerns include strengthening data protection (74.2%), ensuring model integrity (22.6%), improving threat detection and response (48.4%), and investing in workforce training (41.9%) to equip employees for the evolving landscape (**Figure 12**).

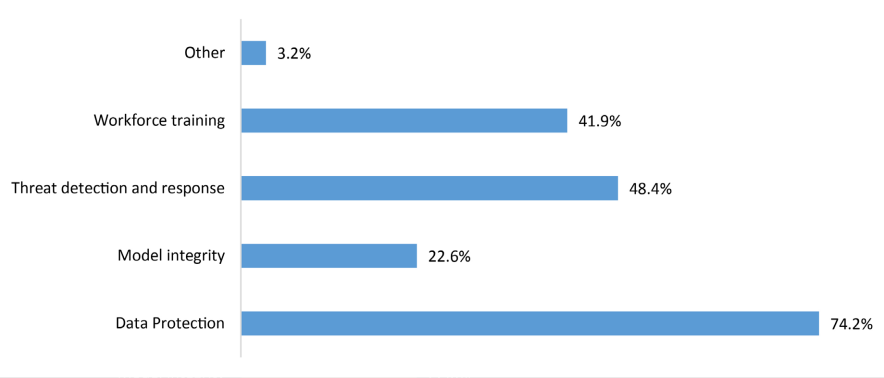

Figure 12. Immediate attention for securing an AI system in the banking sector of Bangladesh.

9. Recommendations

Based on survey findings and global best practices, the following strategies can strengthen AI-driven cybersecurity in Bangladesh's banking sector:

1. Develop AI-Skilled Teams: Hire and train professionals in AI, machine learning, and data analytics, and collaborate with universities to address the talent gap [10].

2. Employee Training: Implement hands-on, scenario-based training to boost confidence in managing AI threats, using simulations and interactive learning [16].

3. Broaden AI Applications: Extend AI beyond security to areas like customer service, credit scoring, fraud detection, and compliance for greater efficiency [4].

4. Optimize AI Systems: Continuously refine AI models through audits, feedback loops, and partnerships with technology providers to stay ahead of evolving threats [8].

5. Strategic Investment: Use phased AI adoption, seek funding, and build partnerships to overcome financial and resource constraints, particularly for smaller banks [14].

6. AI Governance: Align policies with frameworks such as the NIST AI RMF to ensure secure, ethical, and compliant AI use [17].

7. Regulatory Collaboration: Work with regulators to clarify AI policies and invest in advanced cybersecurity tools to counter AI-enabled threats [18].

8. Promote Continuous Learning: Foster a culture of ongoing education to keep staff updated on AI technologies and cybersecurity risks [19]-[22].

10. Conclusion

Banks are increasingly vulnerable to AI-driven cyber threats due to a shortage of skilled professionals, limited employee training, and slow AI adoption. Rapidly evolving attacks such as AI-powered phishing, adaptive malware, and deepfake fraud leave many institutions, especially smaller banks, exposed, risking sensitive data and customer trust. To address this, banks must adopt a proactive approach by expanding AI-focused cybersecurity teams, providing comprehensive staff training, integrating AI across operations, strengthening regulatory frameworks, and fostering industry collaboration. Immediate action is essential to protect data, maintain public confidence, and build resilient defenses that enable the sector to thrive in a digital and interconnected world.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zhang, Y., Wang, J. and Chen, L. (2023) The Transformative Power of AI in Business. *Journal of Business Research*, **154**, 113–124.

[2] World Economic Forum (2023) Global Cybersecurity Outlook. WEF.

[3] Taddeo, M. and Floridi, L. (2018) How AI Can Be a Force for Good. *Science*, **361**, 751-752. https://doi.org/10.1126/science.aat5991

[4] Sharma, P., Kaushik, N. and Tripathi, R. (2022) AI-Enabled Cyber Threats and IoT Vulnerabilities. *IEEE Access*, **10**, 98743–98756.

[5] Rahman, M. and Islam, S. (2021) Cybersecurity Challenges in the Banking Sector of Bangladesh. *Journal of Financial Crime*, **28**, 1250-1265.

[6] PwC (2022) Global Digital Trust Insights. https://www.pwc.es/es/publicaciones/digital/global-digital-trust-2022.pdf

[7] National Institute of Standards and Technology (NIST) (2023) AI Risk Management Framework (AI RMF 1.0). https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

[8] Nguyen, T., Ngo, L.V. and Ruël, H. (2022) Developing Human Capabilities for AI Security: The Role of Training and Learning Culture. *Computers & Security*, **117**, Article 102704.

[9] Mikalef, P., Krogstie, J., Pappas, I.O. and Pavlou, P. (2021) Exploring the Relationship between AI Capabilities and Firm Performance: The Mediating Role of Digital Transformation. *Information & Management*, **58**, Article 103434.

[10] McKinsey & Company (2022) Global AI Adoption Survey. McKinsey.

[11] Kshetri, N. (2021) Cybersecurity and the Changing Threat Landscape. *Computer Law & Security Review*, **43**, 1-10.

[12] Sundaramurthy, S.K., Ravichandran, N., Inaganti, A.C. and Muppalaneni, R. (2022) AI-Powered Operational Resilience: Building Secure, Scalable, and Intelligent Enterprises. *Artificial Intelligence and Machine Learning Review*, **3**, 1-10. https://scipublication.com/index.php/AIMLR/article/view/135

[13] Hubbard, D.W. and Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. Wiley. https://doi.org/10.1002/9781119162315

[14] Hastings, N.B., Young, M. and O'Neill, P. (2023) Building Cybersecurity Talent:

Strategies for Sustainable Workforce Development. *Journal of Cybersecurity Policy and Management*, **8**, 45-63.

[15] Haque, G.M.M., Akula, D.K., Mohammed, Y.S., Syed, A. and Arafat, Y. (2025) Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review. *Emerging Frontiers Library for the American Journal of Engineering and Technology*, **7**, 126-150. http://emergingsociety.org/index.php/efltajet/article/view/255

[16] Deloitte (2023) AI and Risk Management. Deloitte Insights. https://www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/deloitte-gx-ai-and-risk-management.pdf

[17] Creswell, J.W. and Plano Clark, V.L. (2018) Designing and Conducting Mixed Methods Research. 3rd Edition, Sage Publications.

[18] Brynjolfsson, E. and McAfee, A. (2017) Machine, Platform, Crowd: Harnessing Our Digital Future. W.W. Norton & Company.

[19] Braun, V. and Clarke, V. (2006) Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, **3**, 77-101. https://doi.org/10.1191/1478088706qp063oa

[20] Bank of England (2023) AI in Financial Services: Opportunities and Risks. BoE.

[21] Bank for International Settlements (2023) AI Governance in Financial Institutions. BIS.

[22] Bangladesh Telecommunication Regulatory Commission (BTRC) (2023) Cybersecurity Status and Guidelines in Bangladesh. BTRC.

[23] Zetter, K. (2016) That Insane, $81M Bangladesh Bank Heist? Here's What We Know. WIRED. https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/