Roundtable Discussion Series-2026
Keynote Paper of Roundtable Discussion of BIBM
Volume No. 11 , Issue No. 5
2025

# Adoption of AI in Cybersecurity Management of Banks: Bangladesh Perspective

**Md. Shihab Uddin Khan**
*Professor and Director (Research, Development and Consultancy), BIBM*

**Md. Foysal Hasan**
*Assistant Professor, BIBM*

**Fahad Ahmed**
*Lecturer, BIBM*

**S.M. Tofayel Ahmad**
*Additional Director (ICT), Bangladesh Bank*

**Muhammad Abul Kalam Azad**
*Head of Information Security, Eastern Bank PLC*

Published by
**Bangladesh Institute of Bank Management (BIBM)**
**Section No. 2, Mirpur, Dhaka-1216**

Roundtable Discussion Series-2026

Keynote Paper of Roundtable Discussion of BIBM
Volume No. 11, Issue No. 5

# Adoption of AI in Cybersecurity Management of Banks: Bangladesh Perspective

**Md. Shihab Uddin Khan**
*Professor and Director (Research, Development and Consultancy), BIBM*

**Md. Foysal Hasan**
*Assistant Professor, BIBM*

**Fahad Ahmed**
*Lecturer, BIBM*

**S.M. Tofayel Ahmad**
*Additional Director (ICT), Bangladesh Bank*

**Muhammad Abul Kalam Azad**
*Head of Information Security, Eastern Bank PLC*

**Bangladesh Institute of Bank Management (BIBM)**
Mirpur-2, Dhaka-1216, Bangladesh

# Adoption of AI in Cybersecurity Management of Banks: Bangladesh Perspective


**Research Team** **Md. Shihab Uddin Khan**
*Professor and Director (Research, Development and Consultancy) BIBM*
**Md. Foysal Hasan**
*Assistant Professor, BIBM*
**Fahad Ahmed**
*Lecturer, BIBM*
**S.M. Tofayel Ahmad**
*Additional Director (ICT), Bangladesh Bank*
**Muhammad Abul Kalam Azad**
*Head of Information Security, Eastern Bank PLC*

**Editorial Advisor** **Md. Ezazul Islam, Ph.D.**
*Director General, BIBM*

**Editor** **Md. Shihab Uddin Khan**
*Professor and Director (Research, Development and Consultancy), BIBM*

**Support Team** ***Research, Development and Consultancy Wing***
**Papon Tabassum,** *Assistant Senior Officer, BIBM*
**Sk. Md. Azizur Rahman,** *Officer, BIBM*

***Publications-cum-Public Relations Section***
**Md. Al-Mamun Khan,** *Senior Officer (PPR), BIBM*
**Md. Morshadur Rahman,** *Officer (PPR), BIBM*

**Design & Illustration** **Sk. Md. Azizur Rahman,** *Officer, BIBM*



**Published in** May, 2026

**Published by** Bangladesh Institute of Bank Management (BIBM)
Plot No. 4, Main Road No. 1 (South), Section No. 2
Mirpur, Dhaka-1216, Bangladesh.
PABX : +880-48032091-4, 48032097-8, 48032104 (Ext. 135)
+880-58051282
E-mail : bibmresearch@bibm.org.bd
Web : www.bibm.org.bd



**Copyright © BIBM 2026, All Rights Reserved**


*The views in this publication are of authors only and do not necessarily reflect the views of the institutions involved in this publication.*

# Foreword

The banking sector of Bangladesh stands at a critical juncture where traditional security paradigms are being fundamentally challenged by increasingly sophisticated cyber threats. As financial institutions embrace digital transformation and expand their technological footprint, the imperative to safeguard sensitive financial data, maintain customer trust, and ensure operational continuity has never been more pronounced. In this complex and rapidly evolving threat landscape, Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity management, offering unprecedented capabilities in threat detection, response automation, and adaptive defense mechanisms.

In this context, the roundtable discussion paper titled "**Adoption of AI in Cybersecurity Management of Banks: Bangladesh Perspective**" has been prepared and presented on 22 October, 2025 at BIBM. The paper provides a timely and comprehensive examination of how AI is being integrated into the cybersecurity frameworks of Bangladeshi banks. It thoughtfully explores the opportunities, challenges, and practical implications of AI-driven security solutions while addressing the unique technological, regulatory, and organizational contexts that characterize Bangladesh's banking sector.

The insights presented in this paper are particularly relevant for policymakers, banking executives, chief information security officers, IT professionals, regulators, and academicians. By analyzing current adoption patterns, implementation challenges, effectiveness metrics, and future trajectories, the paper contributes to a deeper understanding of how AI-enabled cybersecurity can strengthen resilience, enhance threat intelligence, and support the secure digitalization of banking services.

I commend the efforts of the authors and contributors for their rigorous research approach and scholarly dedication in addressing this vital subject. The intersection of artificial intelligence and cybersecurity represents one of the most significant technological developments in modern banking, and this paper makes a valuable contribution to our understanding of its application within the Bangladesh context.

I am confident that this research will serve as an important reference for stakeholders across the banking ecosystem and will stimulate informed dialogue on building robust, intelligent, and adaptive cybersecurity frameworks. I hope that the findings and recommendations presented herein will contribute meaningfully to policy development, strategic planning, capacity building, and the continued secure digital transformation of our banking sector.

**Md. Ezazul Islam, Ph.D.**
Director General, BIBM

## Acknowledgment

The successful completion of this roundtable discussion paper titled "Adoption of AI in Cybersecurity Management of Banks: Bangladesh Perspective" has been made possible through the collective contributions, cooperation, and encouragement of many individuals and institutions. We express our sincere gratitude to **Dr. Md. Ezazul Islam**, Director General of BIBM, for his continuous guidance and strong support throughout the study.

We are especially thankful to the wider banking community of Bangladesh for their enthusiastic participation and collaboration. The senior officials including Managing Directors/CEOs and Heads of Information Technology and Cybersecurity Departments have generously shared data, insights, and experiences, significantly enriching the analysis and findings of this paper. We would also like to acknowledge the support received from our fellow colleagues at BIBM, especially the teams from the Research, Development and Consultancy (RD&C) Wing, Admin & Accounts Department and Publication-cum-Public Relations Wings, whose cooperation ensured smooth execution of various aspects of the study.

Special appreciation is extended to **Mr. Motahar Hossain**, MBM student at BIBM, for his diligent assistance in data processing and documentation as a research assistant.

Lastly, we are grateful to all those who, directly or indirectly, contributed to this effort. The open discussion and continuous engagement with stakeholders have provided us with diverse perspectives and helped make this paper a comprehensive reflection of the evolving adoption of AI in Cybersecurity Management of Banks in Bangladesh.

**Md. Shihab Uddin Khan**
**Md. Foysal Hasan**
**Fahad Ahmed**
**S.M. Tofayel Ahmad**
**Muhammad Abul Kalam Azad**

# Contents


| | Page |
|---|---|
| Foreword | Iii |
| Acknowledgement | Iv |
| List of Abbreviations | Ix |
| Executive Summary | X |
| 1. Background of the Study | 1 |
| 1.1 Objectives of the Study | 3 |
| 1.2 Research Methodology | 3 |
| 1.3 Structure of the Report | 4 |
| 2. Conceptual Theories of AI in Banking | 4 |
| 2.1 Related Studies on AI in Cybersecurity | 5 |
| 2.2 Bangladesh Bank Guidelines on Utilization of Emerging Technologies (Artificial Intelligence, Machine Learning, Data Analytics, and Robotic Process Automation) and the Management of Associated Security Risks | 7 |
| 3. Global and Local Cases on Effective AI Deployment in Banks' Cybersecurity Management | 11 |
| 4. Data Analysis and Findings | 18 |
| 4.1 Formal AI Adoption Policy for AI-driven Banking Business | 18 |
| 4.2 Formal Internal Policy Regarding the Adoption of AI for Cybersecurity Management | 18 |
| 4.3 Preparedness of Banks' IT Infrastructure for Adopting AI-Driven Cybersecurity Tools | 19 |
| 4.4 Drivers behind the Adoption of AI in Cybersecurity | 20 |
| 4.5 Effectiveness of AI at Identifying and Classifying Cybersecurity Assets and Risks | 21 |
| 4.6 Effectiveness of AI tools at reducing false positives in cybersecurity alerts | 22 |
| 4.7 Effectiveness of AI at Strengthening Protection (e.g., Encryption, Endpoint Security) | 23 |
| 4.8 AI to Automate Access Control and Authentication | 24 |
| 4.9 Applying the Principle of Least Privilege (PLP) for AI Enabled Cybersecurity Data Access | 25 |
| 4.10 AI-powered Tools Used for Anomaly Detection in Cybersecurity | 26 |

Page

4.11 Security Information and Event Management (SIEM) System Uses AI for Real-time Analysis of Security Alerts 26

4.12 Security Operations Center (SOC) uses AI for Threat Correlation and Incident Prioritization in Cybersecurity 27

4.13 AI powered Intrusion Detection Systems (IDS) Integrated into the Bank's Cybersecurity Monitoring 28

4.14 Integration of AI with Intrusion Prevention Systems (IPS) for Real-time Cybersecurity Response 29

4.15 AI for Phishing Detection 30

4.16 Use of AI to Automate Incident Response in Cybersecurity 30

4.17 AI in Post-Incident Cybersecurity Analysis 31

4.18 Level of AI Adoption in Banks for Fraud Detection, Anomaly Detection, and Threat Intelligence 32

4.19 Clarity of Regulatory Frameworks on AI and Cybersecurity in Bangladesh 33

4.20 Collaboration between Banks and Regulators on AI Implementation in Cybersecurity 34

4.21 Implementation of Any Internally Developed AI Tools to Detect and Prevent Anomalies 34

4.22 Current Status of Undertaking Training and Capacity-Building Initiatives 35

4.23 List of Training Programs, Workshops, Or Capacity-Building Initiatives for Bank Officials 35

4.24 Plan to Allocate IT Budget for AI in Cybersecurity 37

4.25 Board of Directors (BoDs) or Senior Executive Management Formally Discussed the Adoption of Ai in Cybersecurity Management 38

4.26 Bank's future plans for AI adoption in cybersecurity 38

4.27 Challenges Banks Face in Adopting AI for Cybersecurity 39

4.28 Summary of Bank Executives' Views on AI Integration in Cybersecurity Management 40

5. Recommendations 41

6. Conclusion 46

References 47

## List of Tables


| | | Page |
|---|---|---|
| Table-01 | Emerging Technology Management | 7 |
| Table-02 | Current Status of Training and Capacity-Building Initiatives Undertaken between 2022 and 2025 | 35 |
| Table-03 | The Names or Titles of Training Programs, Workshops, or Capacity-Building Initiatives | 36 |
| Table-04 | Bank Executives' Views on AI Integration in Cybersecurity Management | 40 |


## List of Figures


| | | |
|---|---|---|
| Figure-01 | Formal AI adoption Policy for AI-driven Banking | 18 |
| Figure-02 | Formal Internal Policy Regarding the Adoption of AI for Cybersecurity | 19 |
| Figure-03 | Preparedness of Banks' IT Infrastructure for Adopting AI-Driven Cybersecurity Tools | 20 |
| Figure-04 | Drivers Behind the Adoption of AI in Cybersecurity | 21 |
| Figure-05 | Effectiveness of AI at Identifying and Classifying Cybersecurity Assets and Risks | 22 |
| Figure-06 | Effectiveness of AI tools at Reducing False Positives in Cybersecurity Alerts | 23 |
| Figure-07 | Effectiveness of AI at Strengthening Protection (e.g., Encryption, Endpoint Security) | 24 |
| Figure-08 | AI to Automate Access Control and Authentication | 24 |
| Figure-09 | Principle of Least Privilege (PLP) for AI enabled Cybersecurity Data Access | 25 |
| Figure-10 | AI-powered Tools Used for Anomaly Detection in Cybersecurity | 26 |
| Figure-11 | SIEM System Uses AI for Real-time Analysis of Security Alerts | 27 |
| Figure-12 | SOC Uses AI for Threat Correlation and Incident Prioritization in Cybersecurity | 28 |
| Figure-13 | AI Powered Intrusion Detection Systems (IDS) Integrated into the Bank's Cybersecurity Monitoring | 28 |
| Figure-14 | Integration of AI with IPS for Real-time Cybersecurity Response | 29 |
| Figure-15 | AI for Phishing Detection | 30 |

Page

Figure-16 Use of AI to Automate Incident Response in Cybersecurity 31
Figure-17 AI in Post-Incident Cybersecurity Analysis 32
Figure-18 AI adoption in Banks for Fraud Detection, Anomaly Detection, and Threat Intelligence 33
Figure-19 Clarity of Regulatory Frameworks on AI and Cybersecurity in Bangladesh 33
Figure-20 Collaboration between Banks and Regulators on AI Implementation in Cybersecurity 34
Figure-21 Plan to Allocate IT Budget for AI in Cybersecurity 37
Figure-22 Board of Directors (BoDs) or Senior Executive Management Formally Discussed the Adoption of AI in Cybersecurity Management 38
Figure-23: Bank's Future Plans for AI Adoption in Cybersecurity 39
Figure-24: Challenges Banks Face in Adopting AI for Cybersecurity 40

## List of Boxes

Box-01: DBS Bank (is Singapore's Leading Bank) - AI/ML in Cybersecurity and Fraud Management 11
Box-02: Visa & AI-driven fraud detection 12
Box-03: Enhancing Cybersecurity Measures at a Global Bank 12
Box-04: Advanced Cyber Defense Initiative at a Reputable Global Bank 13
Box-05: Spear-phishing Attack Prevention at JP Morgan Chase 14
Box-06: Dark Web Monitoring for A Private Commercial Bank 15
Box-07: A Reputed Private Commercial Bank Uses an AI-Powered Threat Detection Tool 17

# List of Abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| APT | Advanced Persistent Threat |
| BB | Bangladesh Bank |
| DA | Data Analytics |
| DL | Deep Learning |
| FCB | Foreign Commercial Bank |
| FEAT | Fairness, Ethics, Accountability, Transparency |
| FGD | Focus Group Discussion |
| IDS | Intrusion Detection Systems |
| IPS | Intrusion Prevention Systems |
| ML | Machine Learning |
| NLP | Natural Language Processing |
| OCR | Optical Character Recognition |
| PCB | Private Commercial Bank |
| PLP | Principle of Least Privilege |
| RPA | Robotic Process Automation |
| SEIM | Security Information and Event Management |
| SDB | Specialized Development |
| SGD | Singapore Dollar |
| SOC | Security Operations Centre |
| SOCB | State-Owned Commercial Bank |
| SSL | Secured Socket Layer |
| TAM | Technology Acceptance Model |
| UEBA | User and Entity Behavior Analytics |
| USD | United States Dollar |
| VPN | Virtual Private Network |
| XAI | Explainable AI |

# Executive Summary

This study provides a comprehensive analysis of the adoption of Artificial Intelligence (AI) in cybersecurity management within the banking sector of Bangladesh, presented in the context of global best practices. The research emphasizes the increasing level of complexity of cyber threats, which specifically target financial institutions because of their systemic significance and sensitive data. Due to the growing inadequacy of traditional cybersecurity techniques, AI-driven systems that can detect threats in real time, perform predictive analytics, and respond automatically must be integrated.

The study adopts a mixed-method research approach, integrating primary and secondary data. Primary data were collected from 38 banks in Bangladesh through semi-structured questionnaires, Focus Group Discussions (FGDs), and expert interviews involving cybersecurity professionals, senior executives, and regulators. Secondary data were drawn from global academic literature, international banking case studies, regulatory guidelines, and industry reports. The qualitative findings reveal a persistent perception gap at the senior management level. At the same time, most boards have formally discussed AI adaptation in cybersecurity management, and many executives continue to misjudge the urgency and return on investment. Bangladesh Bank's ICT Security Guidelines (Version 4.0, 2023) provide a framework for managing risks associated with AI, machine learning, data analytics, and robotic process automation.

Global case studies illustrate the transformative potential of AI when deployed at scale. For instance, DBS Bank in Singapore deployed over 800 AI/ML models across 350 use cases, generating SGD 370 million in economic benefit in 2023, while Visa prevented 80 million fraudulent transactions worth $40 billion using AI-driven fraud detection. These examples demonstrate that AI can materially reduce fraud, enhance compliance, and improve operational efficiency when supported by strong governance and ethical frameworks.

The survey revealed that AI adoption in Bangladesh's banking sector is still at an early and growing stage. Many banks are not yet fully ready, and their plans and strategies are not well aligned. Only 32% of banks have formal AI policies, and just 23% have specific policies for using AI in cybersecurity. In terms of readiness,

only 11% of banks are fully prepared, while 69% are partially prepared, which means there are still gaps in technology and infrastructure.

AI is mainly used in areas like threat detection and response. About 81% of banks said that rising cyber threats are the main reason for using AI. Around 73% of banks believe AI is helpful in identifying risks, and 51% said it helps reduce false alerts. However, use in advanced areas is still low. Only 51% use AI for phishing detection, 46% have no automated incident response, and 62% have not used AI in access control systems. Still, some banks have started using AI in fraud detection and chatbot-based customer service, which has improved anomaly detection and customer trust.

Banks face several challenges, such as high costs, old systems, and a lack of skilled professionals. Many banks also do not have proper AI training programs, and existing training is not enough to handle cybersecurity needs. This weakens both skills and overall readiness. Therefore, banks need better and more structured training programs. Despite these challenges, 70% of banks plan to expand AI use, showing that they understand its importance for better security, efficiency, and customer confidence.

The results confirm that while Bangladeshi banks are aware of AI's potential, adoption remains fragmented and slow. To accelerate progress, policymakers and executives must prioritize investment in infrastructure, workforce training, and regulatory alignment. By bridging the gap between global best practices and local readiness, Bangladesh's banking sector can harness AI to strengthen digital resilience, enhance customer trust, and secure its competitive position in the global financial landscape.

# Adoption of AI in Cybersecurity Management of Banks: Bangladesh Perspective

## 1. Background of the Study

The digital era has undoubtedly fostered significant technological innovation; however, it has simultaneously introduced new and evolving cybersecurity threats. Cyberattacks are becoming increasingly sophisticated and persistent, targeting machines, enterprises, and critical infrastructure with growing frequency and intensity.

The cybersecurity community has strongly focused on attack detection as a cornerstone strategy in response to the growing threats. This approach comprehensively monitors network activities, system status, and usage patterns to pre-emptively identify and neutralize unauthorized access or attacks. Within this landscape, Artificial Intelligence (AI) and its subsets, including ML and DL, offer promising solutions to support cybersecurity. AI's capacity to rapidly evolve and handle large datasets makes it well-suited for identifying and responding to sophisticated cyber threats. By analyzing patterns and learning from experience, AI-based systems can detect malware, insider threats, botnets, network intrusions, phishing attempts, and other malicious activities (Parizad &, Hatziadoniu, 2022).

Security concerns have intensified in the banking sector amidst the proliferation of digital transactions and cyber threats (Aripin, 2024). The banking sector has long been a target for cybercriminals due to the highly sensitive and valuable nature of the information it handles. With digitalization accelerating globally, banks are increasingly reliant on technology, which has expanded their digital footprints but also exposed them to complex cybersecurity threats. The traditional methods of managing cybersecurity are often inadequate in dealing with modern cyberattacks, which are becoming more sophisticated, frequent, and varied. As a result, financial institutions are looking at Artificial Intelligence (AI) as a means of enhancing their cybersecurity posture. AI-driven solutions

have the potential to transform cybersecurity by providing advanced capabilities such as real-time threat detection, predictive analytics, automated responses, and adaptive learning mechanisms. These AI systems can analyze vast amounts of data to identify patterns, detect anomalies, and respond to threats more quickly and accurately than human analysts alone.

The banking industry in Bangladesh has undergone a rapid digital transformation, driven by enhanced internet accessibility, the emergence of digital payment methods, and governmental initiatives promoting a digital economy. Although these advancements have increased customer convenience and improved operational efficiencies, they have simultaneously exposed banks to a new array of cybersecurity threats. Cyberattacks aimed at financial institutions in Bangladesh have escalated in recent years, presenting considerable challenges to the security of financial information and the integrity of banking operations.

Notwithstanding these obstacles, the integration of AI in cybersecurity management among Bangladeshi banks remains in its early phases. A lack of awareness among bank employees and relevant stakeholders, a perception gap among senior management, elevated costs, and a deficiency of professionals skilled in AI are several of the challenges impeding the extensive adoption of AI-based cybersecurity strategies in our banking industry.

This paper seeks to explore the adoption of AI in cybersecurity management within the banking sector, with a focus on the current state, challenges, and potential impacts of AI technologies. It examines how the banks are utilizing AI to detect, prevent, and mitigate cybersecurity threats, and whether these technologies are effective in strengthening their overall security posture. The study also addresses the unique challenges faced by Bangladeshi banks in adopting AI, including issues related to data privacy, regulatory compliance, and resource constraints. By analyzing both quantitative data from surveys and qualitative insights from interviews and FGD with industry experts and practitioners, this research aims to provide a comprehensive overview of AI's role in cybersecurity management in Bangladeshi banks.

The findings of this research will have significant implications for policymakers, bank executives, and cybersecurity professionals in Bangladesh. By understanding the potential of AI in enhancing cybersecurity, stakeholders can make informed decisions regarding investment in AI technologies, policy formulation, and capacity building. Furthermore, the study will contribute to the broader discourse on digital transformation in the financial sector, highlighting the importance of AI as a strategic asset for cybersecurity. As cyber threats continue to evolve in complexity and diversity, the demand for innovative and adaptive cybersecurity solutions becomes ever more crucial. This research underscores the urgency for Bangladeshi banks to embrace AI not only as a tool for cybersecurity but also as a key enabler of their digital resilience and competitive advantage in a rapidly changing landscape.

### 1.1 Objectives of the Study

This paper examines the potential of Artificial Intelligence (AI) in the domain of cybersecurity management in the banking context of Bangladesh. The specific objectives of this paper are **one,** discussing the conceptual issues of Artificial Intelligence in the domain of Cybersecurity; **two,** observing global scenario of the use of AI in cybersecurity; **three,** showing the existing practices of using AI in cybersecurity management of banks; and **four,** identifying the key challenges and opportunities associated with the AI adoption in cybersecurity for our banking systems; and **finally,** develop a set of recommendations for accelerating AI adoption in the cybersecurity landscape of Bangladeshi banks.

### 1.2 Research Methodology

This report uses both primary and secondary data. Primary data were collected through a semi-structured questionnaire from the Information Security wing/cell of banks. A questionnaire was sent to all banks in Bangladesh. We received data from 38 banks (**Annexure-I**). Among the respondent banks, there were 3 State-Owned Commercial Banks (SOCBs), 3 Foreign Commercial Banks (FCBs), 30 Private Commercial Banks (PCBs), and 2 Specialized Development Banks (SDBs). The secondary data

were collected from websites, published articles, newspapers, and the internet. Focus Group Discussions (FGD), online and in-person interviews were also employed to gather data.

### 1.3 Structure of the Report

The paper is organized into five sections. The **first section** outlines the introduction, objectives, methodology, and structure of the report; **section two** reviews the literature, conceptual issues and regulatory policies on Artificial Intelligence and Cybersecurity in banking; **section three** shares both global and local cases on AI adoption in cybersecurity domain in the banks; **section four** presents a comprehensive analysis of the surveyed data concerning the potential applications and opportunities of AI in the cybersecurity of banks; **finally, section five** provides recommendations or suggestions for the effective integration of AI in the cybersecurity of banks.

## 2. Conceptual Theories of AI in Banking

Artificial Intelligence (AI) is changing how banks work and think. It helps banks use data to make quicker and safer decisions. AI systems can learn from past cases, adapt to new data, and act with less human help. In Bangladesh, banks are slowly using these tools to manage cyber risks more smartly. AI in banking runs mainly on Machine Learning (ML) and Deep Learning (DL). ML uses past data, like customer records, to find patterns and predict risks. It can warn when a transaction looks odd or when fraud might occur. DL goes deeper. It uses layered networks, much like the human brain, to find complex patterns that old systems often miss (Hernández Aros et al., 2024). These tools help banks spot hidden threats and act faster.

Another growing field is Agentic AI. It gives systems the power to act on their own. An Agentic AI can watch live transactions, detect suspicious activity, and trigger safety steps without waiting for people to respond. This cuts the delay and helps banks react in real time. Natural Language Processing (NLP) helps computers understand and use human language. In banks, it powers chatbots, scans reports, and checks documents for errors. NLP tools can also catch fake emails and phishing links before users click

them (Jabbar, 2025). When combined with data models, NLP helps banks make better and faster security decisions.

AI now plays a central role in cyber defense. Banks use AI in Security Information and Event Management (SIEM) and Security Operations Centers (SOC). These systems gather large amounts of data and flag risky behavior (González-Granadillo et al., 2021). Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have also become smarter. Instead of looking only for known attacks, AI-powered systems study normal activity. They spot anything that seems out of line and block it (Pinto et al., 2023). Reinforcement Learning adds another layer of strength. It helps phishing detection tools learn from new tricks used by hackers. Each time attackers change methods, the system adjusts (Jabbar, 2025). Even with all this progress, people still matter. AI can point out risks, but humans must decide what to do. The Behavioral Decision Theory reminds us that judgment and trust come from people, not machines (Khadka & Ullah, 2025).

In Bangladesh, not all banks have the same technology level. The real test is how well staff can use AI insights and make sound calls. Training, trust, and clear roles are vital for success. AI should help people think better, not replace them. AI in banking works best when people and machines support each other. The goal is not just automation but improvement. When banks use AI wisely, they can predict risks, stop fraud early, and build stronger defenses.

### 2.1 Related Studies on AI in Cybersecurity

AI is changing how banks manage cyber risks. It shifts cybersecurity from reacting after attacks to predicting and preventing them. Mohamed (2025) shows that AI helps in intrusion detection, malware detection, insider threat control, and automated response. Traditional signature-based tools fail against new or zero-day attacks. Machine Learning (ML) and Deep Learning (DL) models can study normal network patterns, detect odd activity, and isolate affected systems quickly, often cutting response time by more than 70 percent.

Fraud detection is one of the most common uses of AI in banking. Hernández Aros et al. (2024) found that ML models can identify unusual transaction behavior and detect new fraud types. Pinto et al. (2023) reported that ML-based intrusion systems can spot abnormal activity in real time. González-Granadillo et al. (2021) noted that DL in Security Information and Event Management (SIEM) systems reduces false alerts and identifies complex attacks more accurately. Jabbar (2025) showed that using Natural Language Processing (NLP) with reinforcement learning helps catch phishing emails and links before users open them, protecting both customers and employees. Explainable AI (XAI) is gaining interest because it makes AI decisions easier to understand. Rjoub et al. (2023) explained that XAI helps banks and regulators trust AI-driven security tools and comply with standards. Krishnamurthy and Vemulapalli (2024) discussed the use of generative AI in cybersecurity and stressed the need for human oversight to ensure ethical and transparent use of automated tools.

In Bangladesh, research shows that AI use in banking security is growing but still limited. Rahman and Akter (2025) found that AI-based protection systems improve user trust in online banking. Using the Technology Acceptance Model (TAM), they showed that customers feel safer when banks use AI to protect their data. LightCastle Partners (2024) observed that some banks have started testing AI tools for fraud detection and chatbots, but large-scale use remains rare. The main barriers are high cost, outdated systems, and lack of quality data. Khan et al. (2024) reported that only about 6 percent of banks are fully ready for AI adoption. They highlighted low awareness, limited budgets, and weak regulations as major obstacles.

Together, these studies show two clear trends. Global research proves that AI makes cybersecurity more predictive, adaptive, and efficient (Mohamed, 2025; Hernández Aros et al., 2024; Pinto et al., 2023; González-Granadillo et al., 2021; Jabbar, 2025). Local studies highlight the need for readiness, policy support, and skilled professionals (Rahman & Akter, 2025; LightCastle Partners, 2024; Khan et al., 2024). A concise summary of the related studies is presented in **Annexure-II**.

Although Bangladesh is still in the early phase, its banks are becoming aware of AI's potential for fraud detection, network protection, and customer safety. The key challenge is not the lack of AI tools but the limited capacity to adopt and manage them. Building trust, training staff, and setting clear regulations will be critical to accelerate adoption. These insights link directly to this research, which explores how Bangladeshi banks can adopt AI in cybersecurity management to improve protection, compliance, and operational trust.

### 2.2 Bangladesh Bank Guidelines on Utilization of Emerging Technologies (Artificial Intelligence, Machine Learning, Data Analytics, and Robotic Process Automation) and the Management of Associated Security Risks

According to the Bangladesh Bank ICT Security Guidelines (Version 4.0, 2023), the security risks associated with the adoption of AI in banks are outlined in Chapter 14 (Emerging Technology Management). The Table - 01 presents the pertinent clauses related to the management of emerging technology issues as specified in the BB Guideline.

| **Table-01: Emerging Technology Management** | |
|---|---|
| **14.1 Artificial Intelligence (AI)** | |
| **14.1.1 AI Security Risks** | AI is a relatively new force in business; thus, AI enablers, or the AI itself, could create new risks. As well as, AI has significant challenges for organizations, from reputational damage and revenue losses to regulatory backlash, criminal investigation, and diminished public trust. AI systems may have scripting errors, flawed algorithms, data difficulties, or lapses in data management, technology, and process troubles/issues, security snags, and inadequate human-machine interactions. They may also deliver biased results, and an underrepresented data population may be used to train the AI model. |
| **14.1.2 AI Security Management** | i. Rigorous safeguards shall be ensured so that disgruntled employees or external foes cannot corrupt algorithms or use an AI application in malicious ways. |

| | |
|---|---|
| | ii. Human judgment shall be applied to prove faulty system results, biased results, or models' misbehavior.<br>iii. AI models shall be transparent for improved customer service.<br>iv. AI systems shall be continuously monitored and operated by qualified human resources.<br>v. Sensitive information like Personally Identifiable Information (PII) may be hidden among anonymous data. Thus, the AI system shall be designed so that sensitive information is challenging to reveal (if any).<br>vi. "Relevant Employees shall be well trained on working knowledge of AI systems, shall have awareness of related risks and mitigation actions," as not all employees may need working knowledge.<br>vii. The Organization shall conduct scenario planning and create a fallback plan to handle disaster situations; in such cases, AI model performance drifts, data inputs shift unexpectedly, or sudden changes, such as a natural disaster occur in the external environment. |
| **14.2 Machine Learning (ML)** | |
| Machine learning for financial forecasting can be applied to many administrative, operational, and client areas of the banking industry. Artificial Intelligence and Machine Learning can provide unprecedented levels of automation, either by taking over the tasks of human experts or by enhancing their performance while assisting them with routine and repetitive tasks. Organizations benefit from machine learning; some common uses are facial recognition and Optical Character Recognition (OCR) technology. | |
| **14.2.1 ML Security Risks** | Machine learning systems open new avenues for attacks that don't exist in conventional procedural programs. One of these is the evasion or adversarial attack, in which a foe attempts to inject inputs to ML models intentionally to trigger mistakes. The data may look okay to humans, but subtle variances can cause ML algorithms to go wildly off track. |

| | |
|---|---|
| | Such attacks may occur at inference time by exploiting the model's internal information, typically in white and black-box attacks. The most common machine learning attacks are Evasion, Poisoning, Model Inversion, Online System Manipulation, Transfer learning, and Privacy Attacks. |
| **14.2.2 ML Security Management** | i. A mechanism or plan shall be developed to inspect the training data for contamination when training is done internally.<br>ii. Ground-truth tests shall be performed on the model after every training session. Significant changes in classifications from the original collection will show poisoning.<br>iii. The model shall be compressed to become a smooth decision surface, resulting in less room for an attacker to manipulate it.<br>iv. The model shall be trained with all the possible accusatory examples an assailant can use.<br>v. The algorithm shall not be biased. |
| **14.3 Data Analytics (DA)** | |
| Today, success is achieved by driving intelligent customer engagement based on a data-driven understanding of the business. Technology and digitization have transformed the financial sector by enabling it with real-time actionable insights to make informed decisions, creating competitive advantages, and elevating consumer experience. DA also allows the Organizations to share potential products, upsells, cross-sells, and strategic planning with customers. With AI-backed models, the ability to transform customers' banking experiences is exponential. | |
| **14.3.1 DA Security Risks** | Data Tampering, Eavesdropping, Data Theft, Falsifying User Identities, password-related threats, Unauthorized Access to Tables and Columns or Data Rows, and Lack of Accountability are some loopholes in data analytics. |
| **14.3.2 DA Security Management** | i. The analyst shall be well-versed in all stages of Data Analytics and Data Analysis tools and techniques. |

| | |
|---|---|
| | ii. Adequate monitoring may consider the activities related to the systems and user behavior, especially potentially suspicious patterns or behavioral trends, to keep threats away.<br>iii. Tracking of User Access shall be established. At regular intervals, Access should be reviewed.<br>iv. Sensitive Files shall be restricted.<br>v. Behavior-based permissions shall be established.<br>vi. Data sanitization shall be in place.<br>vii. Data Analysts shall report analysis results in a clear and understandable form. |
| **14.4 Robotic Process Automation (RPA)** | |
| Robotic Process Automation improves the user experience by allowing bots to handle repetitive tasks without human intervention to provide better customer service. | |
| 14.4.1 | Accountability for Bot actions shall be ensured. |
| 14.4.2 | Bot operators and Bot identities shall be differentiated. |
| 14.4.3 | RPA implementation can lead to an increase in account privileges and fraud. Thus, RPA access shall be strictly restricted to what each Bot needs to conduct the assigned task. |
| 14.4.4 | The RPA tool shall provide complete, system-generated logs without any gaps. |
| 14.4.5 | The integrity of the RPA logs shall be protected to aid proper investigation or review in case RPA security fails or an incident happens. |
| 14.4.6 | Periodically, reviews and tests shall be conducted on RPA scripts focusing on business logic vulnerabilities. |

**Source**: BB ICT Security Guideline, Version 4.0, 2023

## 3. Global and Local Cases on Effective AI Deployment in Banks' Cybersecurity Management

AI is increasingly used by banks to enhance cybersecurity, detect fraud, and monitor suspicious activities in real time. This chapter presents some cases from both global and local banks/FIs to show how AI is applied effectively in various financial services or functions. It highlights successful strategies, key benefits, and challenges faced during the implementation process.

**Box-01: DBS Bank (is Singapore's Leading Bank) - AI/ML in Cybersecurity and Fraud Management**

"DBS Bank has significantly advanced its cybersecurity and fraud detection capabilities through the integration of Artificial Intelligence (AI) and Machine Learning (ML). In 2023, the bank deployed over 800 AI/ML models across more than 350 use cases, generating an economic benefit of Singapore Dollars, SGD 370 million, more than double the value achieved in 2022.

A major application is in real-time digital fraud detection, where AI-driven solutions analyze transaction data and flag potentially fraudulent activities in under 10 milliseconds. This has improved scam detection accuracy, reduced false positives, and enhanced operational efficiency. The AI/ML models also support Anti-money Laundering (AML), risk assessment, and sanctions compliance, enabling the bank to proactively mitigate cyber threats and financial crime risks.

To ensure ethical and responsible AI deployment, DBS adheres to the FEAT framework (Fairness, Ethics, Accountability, Transparency), guiding AI model development and deployment while maintaining regulatory compliance and customer trust. Governance is supported by cross-functional committees overseeing high-risk decisions and ensuring alignment with internal policies and MAS guidelines.

Overall, DBS Bank demonstrates that large-scale, ethically governed AI deployment can materially improve cybersecurity, fraud prevention, and risk management outcomes in modern banking."

**Source**: DBS Bank, *Annual Report 2023 – CIO Statement*, DBS Bank Limited, Singapore, 2023.

**Box-02: Visa & AI-driven fraud detection**

"In banking and online payments, AI is used to detect fraud by monitoring transaction patterns and user behavior in real-time. Machine learning models analyze factors like spending habits, login locations, device identifiers, and transaction anomalies to flag potentially fraudulent activities (e.g., credit card theft, account takeover, money laundering). Unlike static rules, AI systems continuously adapt to new fraud tactics and can catch subtle irregularities across millions of transactions.

In 2023, Visa leveraged AI to prevent 80 million fraudulent transactions totaling $40 billion. Its AI models assess transaction risk in milliseconds, detecting anomalies such as unusual charges or spending patterns before they impact customers.

Major banks utilize similar AI systems to monitor logins and fund transfers, flagging events such as large transactions from unfamiliar locations or devices. These tools often enable real-time fraud prevention by freezing suspicious activity and notifying analysts.

Visa's case highlights how AI has become a central component in fraud mitigation across the financial sector."

**Source**: https://research.aimultiple.com/ai-cybersecurity-use-cases/

**Box-03: Enhancing Cybersecurity Measures at a Global Bank**

**Challenge**

"A Global Bank identified an increasing trend in sophisticated cyber threats targeting the financial sector. These threats included advanced persistent threats (APTs), phishing attacks, and ransomware aimed at stealing sensitive customer data and disrupting financial operations. The nature of these attacks not only threatened the privacy and assets of the bank's clients but also posed severe risks to the bank's reputation and operational stability. The challenge was compounded by the bank's vast digital footprint and the need to comply with stringent regulatory requirements across different jurisdictions.

**Solution**

The Bank launched an extensive cybersecurity overhaul to tackle these emerging threats effectively. The cornerstone of this initiative was establishing a next-

generation Security Operations Center (SOC) equipped with the latest threat intelligence and incident response technologies. The bank employed artificial intelligence algorithms to swiftly identify irregular patterns and security lapses, outpacing traditional detection methods. Furthermore, the Bank implemented multi-factor authentication and end-to-end encryption across all digital platforms to secure client transactions and data. They initiated a comprehensive employee education initiative centered on enhancing cybersecurity awareness and promoting security best practices. Strategic partnerships with leading cybersecurity firms allowed the bank to stay ahead of emerging cyber threats through continuous updates and adaptive security measures.

**Result**

Implementing these advanced cybersecurity measures has significantly enhanced the bank's defensive capabilities. The bank observed an 80% reduction in successful phishing attempts and a substantial decrease in vulnerability exploits. The strengthened security protocols improved compliance with global financial regulations, minimizing legal and financial risks associated with cyber incidents. This proactive cybersecurity strategy protected customers' assets and reinforced the reputation as a secure and trustworthy institution. The successful overhaul of their cybersecurity landscape has set a new industry standard, showcasing the critical importance of cybersecurity in safeguarding the financial sector's integrity."

**Source**: https://digitaldefynd.com/IQ/banking-cybersecurity-case-studies/

**Box-04: Advanced Cyber Defense Initiative at a Reputable Global Bank**

**Challenge**

"A Reputed Global Bank identified a significant vulnerability in its cyber defenses, primarily due to outdated security infrastructure and the increasing sophistication of cyberattacks targeted at the financial sector. These vulnerabilities were particularly acute in mobile banking and digital payments, where the intersection of high transaction volumes and sensitive customer data presented attractive targets for cybercriminals. The bank needed to address these challenges to prevent potential data breaches, financial fraud, and loss of customer trust.

**Solution**

The Bank embarked on an ambitious project to modernize its cybersecurity infrastructure. This project focused on enhancing digital payment security by implementing state-of-the-art cryptographic solutions and secure socket layer (SSL) protocols to protect data in transit. The bank also adopted cloud-based security solutions, providing scalable and robust defenses against various cyber threats.

An integral part of their strategy was the introduction of an AI-driven security platform that leveraged machine learning to detect and respond to security anomalies in real-time. The Bank also established a new protocol for rapid incident response and recovery, which included automated systems for immediate threat neutralization and recovery processes to minimize downtime and service disruption. To ensure the effectiveness of these technological tools, the Bank invested in comprehensive training programs for all employees, focusing on cybersecurity best practices and the importance of maintaining a secure digital environment. The bank also initiated regular security audits and penetration testing conducted by external experts to continuously assess and refine its security measures.

**Result**

The cybersecurity overhaul at the Bank yielded substantial improvements. The enhanced security measures significantly reduced the incidence of cyber-attacks, with a reported decrease of over 85% in attempted data breaches. The advanced security protocols around digital payments fortified the bank's defenses against transactional fraud, instilling greater confidence among clients using digital banking services. The Bank's proactive approach safeguarded its operational integrity and client data and reinforced its reputation as a leader in banking security within the financial industry."

**Source**: https://digitaldefynd.com/IQ/banking-cybersecurity-case-studies/

**Box-05: Spear-phishing Attack Prevention at JP Morgan Chase**

**Challenge**

"In an age characterized by advanced cyber threats, JP Morgan Chase encountered a formidable obstacle in the form of targeted spear-phishing attacks. These attacks involved highly targeted and deceptive communications

that aimed to trick employees into exposing sensitive information such as login credentials and access to financial systems. Given the sophisticated nature of these attacks, they represented a potent threat to the integrity of the bank's security protocols, posing risks of data breaches, financial loss, and considerable damage to its reputation.

**Solution**

JP Morgan Chase adopted a comprehensive and proactive approach to mitigate spear-phishing risks. The cornerstone of this strategy was implementing an advanced email security system that utilized state-of-the-art Machine Learning (ML) algorithms to identify and filter out malicious emails. This system could analyze email content for phishing indicators, thereby preventing many attacks before they could reach employee inboxes.

Alongside technological solutions, JP Morgan Chase bolstered its defenses through employee education. The bank instituted a widespread cybersecurity awareness program that included regular training sessions, simulations of phishing scenarios, and communications on the latest phishing techniques and trends. This program aimed to equip employees with the necessary skills and knowledge to effectively recognize and report phishing attempts.

**Result**

At JP Morgan Chase, the successful execution of sophisticated email filtering technology alongside extensive employee training resulted in a significant reduction in both the frequency and impact of spear-phishing attacks targeting the bank. This two-pronged defense mechanism safeguarded crucial data and fostered a culture of cybersecurity consciousness and alertness among the employees. This proactive stance on cybersecurity reinforced JP Morgan Chase's reputation as a secure and trustworthy financial institution committed to protecting its stakeholders from emerging cyber threats."

**Source**: https://digitaldefynd.com/IQ/banking-cybersecurity-case-studies/

## Local Cases (Bangladeshi Banks)

**Box-06: Dark Web Monitoring for A Private Commercial Bank**

"A leading financial institution in Bangladesh manages sensitive data, including customer identification records (such as NID and passport details), financial transactions, employee credentials, and internal proprietary information. Its cybersecurity environment is challenged by evolving threats such as phishing,

identity theft, credential leaks, fraud, and impersonation, requiring robust monitoring and defense mechanisms to safeguard its assets and customer trust.

To proactively detect when the bank's sensitive data, intellectual property, or brand appears on the dark web or in illicit marketplaces/forums so that the bank can respond swiftly, contain damage, reduce financial and reputational loss, and comply with regulations.

**Key Activities Features Relevant to the Bank**

- Continuous scanning of dark web / deep web sources (e.g., TOR, I2P, paste sites, underground forums) for leaked credentials, personal data, financial data, and card data.
- AI/NLP-powered analysis to filter and classify risk: identifying high-risk leaks vs noise, detecting threat actor discussions about planning attacks, or selling stolen data.
- Real-time or near-real-time alerts for critical data are triggered by systems that monitor and analyze banking activities instantly. These systems use technologies like AI and machine learning to detect anomalies, fraud, or other suspicious events as they happen, enabling banks to immediately flag or halt transactions and notify customers or internal teams. Key technologies include complex event processing, which correlates data across multiple streams, and real-time analytics, which process vast amounts of data per second to spot risks and unusual patterns.
- Brand/executive monitoring: detection of impersonation (fake domains, fake social media profiles), leaks involving executive PII.
- Compromised cards detection, where fraud/card data may be compromised or sold.
- Integration with other security systems/workflows: e.g., SIEM, incident response, vulnerability management."

**Source**: Collected through discussion from the Cybersecurity unit of a reputed Bank, 2025.

**Box-07: A Reputed Private Commercial Bank Uses an AI-Powered Threat Detection Tool**

"The Bank leverages the AI capabilities of SIEM to identify cyber threats in real time across its entire digital ecosystem—including core banking systems, ATMs, online and mobile banking platforms, and internal networks. SIEM uses multiple layers of AI and automation to enhance alert enrichment, threat prioritization, and incident correlation. The objective is to detect both known and zero-day attacks early while minimizing manual effort and improving response accuracy. Given the bank's massive volume of log data generated from firewalls, endpoints, network devices, and cloud systems, traditional rule-based monitoring is often insufficient resulting in alert fatigue and delayed threat detection. AI-driven analytics facilitate quicker and more intelligent identification and response to threats. To achieve this, the Bank incorporates AI-powered correlation and machine learning (ML) models to improve the capabilities of its Security Operations Center (SOC).

**AI-Driven Correlation Engine**

- SIEM uses an AI-augmented correlation engine that analyzes massive log streams in real time.
- Instead of relying solely on predefined static rules, AI dynamically correlates related events across multiple systems — such as firewalls, VPNs, authentication servers, and applications.

This correlation logic is continuously optimized through machine learning, allowing the system to detect even those attacks that do not match any known signature.

By utilizing AI-driven threat detection, SIEM allows the Bank to shift its cybersecurity operations from a reactive log analysis approach to a proactive and intelligent defense strategy. The system's capacity to learn, adapt, and correlate intricate event patterns guarantees that potential threats are recognized and addressed in real time, thereby protecting the bank's digital infrastructure, customer information, and reputation."

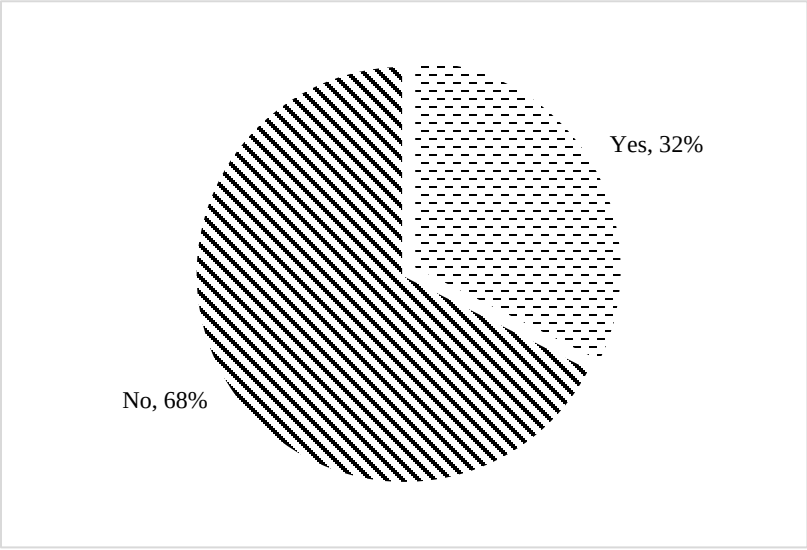
**Source**: Collected through discussion from the Cybersecurity unit of a reputed Bank, 2025.

## 4. Data Analysis and Findings

### 4.1 Formal AI Adoption Policy for AI-driven Banking Business

The survey data indicates that only 32 percent of banks currently have a formal AI adoption policy for AI-driven banking business. Conversely, the majority, approximately 68 percent, do not have any formalized guidelines in place. This highlights a significant gap in strategic governance and risk management related to AI deployment in the banking sector.

**Figure-01: Formal AI Adoption Policy for AI-driven Banking**

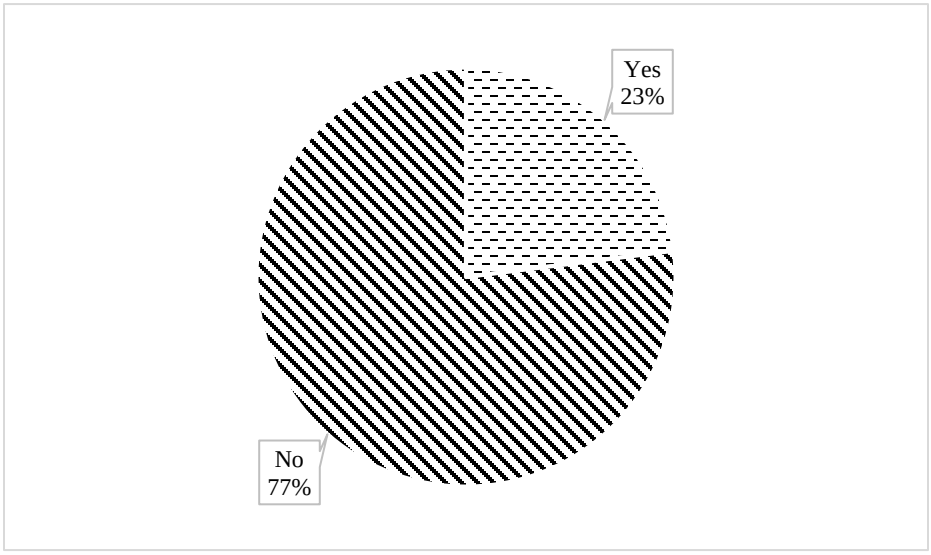



**Source**: BIBM Survey

### 4.2 Formal Internal Policy Regarding the Adoption of AI for Cybersecurity Management

The survey data indicates that approximately 23 percent of banks have established a formal internal policy regarding the adoption of AI for cybersecurity purposes**,** while the remaining 77 percent have not. This suggests that a majority of banks are still in the early stages of formalizing AI governance within their cybersecurity strategies.

**Figure-02: Formal Internal Policy Regarding the Adoption of AI for Cybersecurity**

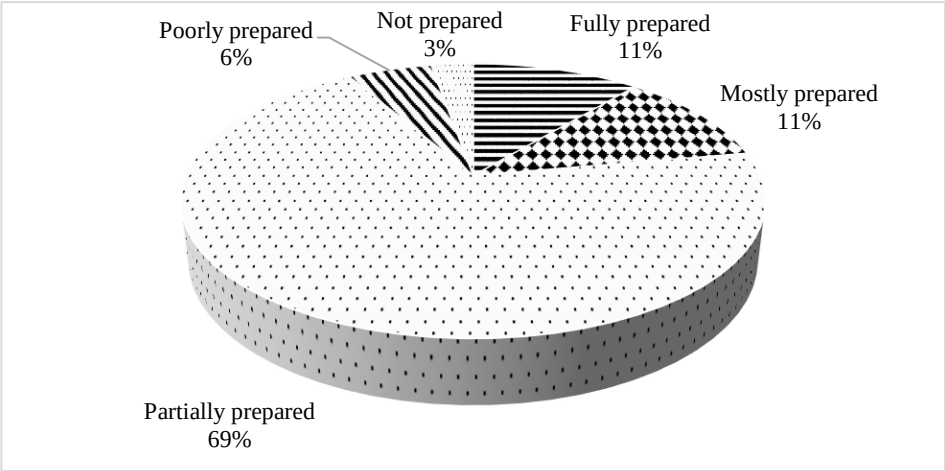



**Source**: BIBM Survey

### 4.3 Preparedness of Banks' IT Infrastructure for Adopting AI-Driven Cybersecurity Tools

Figure 3 illustrates the preparedness level of banks' IT infrastructure for adopting AI-driven cybersecurity tools. The result reveals that a majority (69%) of the surveyed banks reported being partially prepared, indicating that while foundational systems and awareness exist, significant improvements are still required to achieve full readiness. A smaller proportion, 11 percent of banks, considered themselves mostly prepared, suggesting that they are in the advanced stages of readiness but may still face certain technical or operational gaps. Similarly, another 11 percent identified themselves as fully prepared, demonstrating that a few institutions have achieved a mature IT infrastructure capable of integrating AI-based cybersecurity solutions effectively. In contrast, 6 percent of respondents reported being poorly prepared, and 3 percent stated they were not prepared at all.

**Figure-03: Preparedness of Banks' IT Infrastructure for Adopting AI-Driven Cybersecurity Tools**



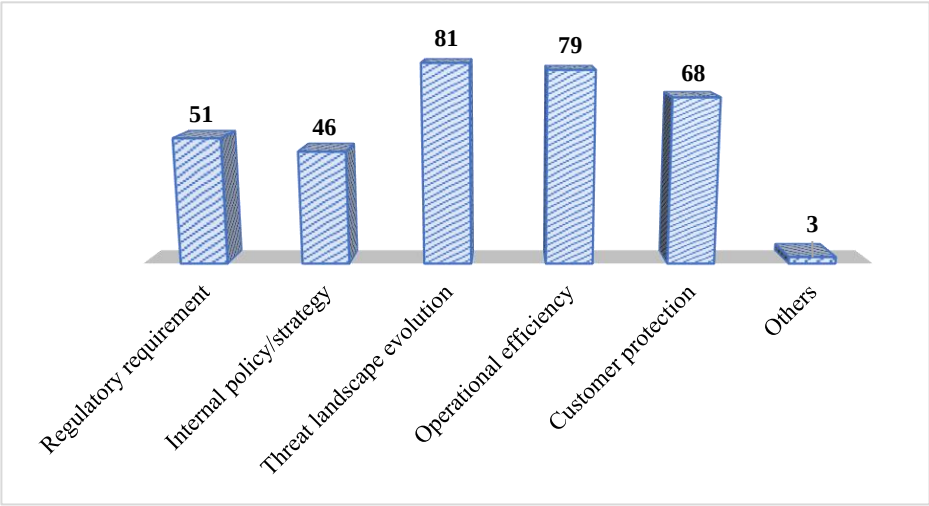

**Source**: BIBM Survey

### 4.4 Drivers behind the Adoption of AI in Cybersecurity

Figure-4 demonstrates the primary drivers influencing the adoption of Artificial Intelligence (AI) in cybersecurity across the banking sector. The findings reveal that the evolution of the threat landscape is the most significant driver, cited by 81 percent of respondents. This underscores the growing recognition among banks that conventional cybersecurity measures are insufficient to counter increasingly sophisticated and dynamic cyber threats. The second most influential factor is operational efficiency (79%), reflecting the sector's emphasis on leveraging AI to enhance automation, speed, and accuracy in threat detection and incident response.

Customer protection also emerged as a major motivating factor, with 68 percent of respondents indicating that safeguarding clients' financial assets and personal data is a key consideration for adopting AI-driven cybersecurity solutions. Additionally, regulatory requirements (51%) and internal policy or strategy alignment (46%) were identified as moderate drivers, suggesting that compliance obligations and institutional strategies are playing an increasingly important role in shaping cybersecurity decisions. A small proportion **(**3%**)** cited other miscellaneous factors.

**Figure-04: Drivers behind the Adoption of AI in Cybersecurity**

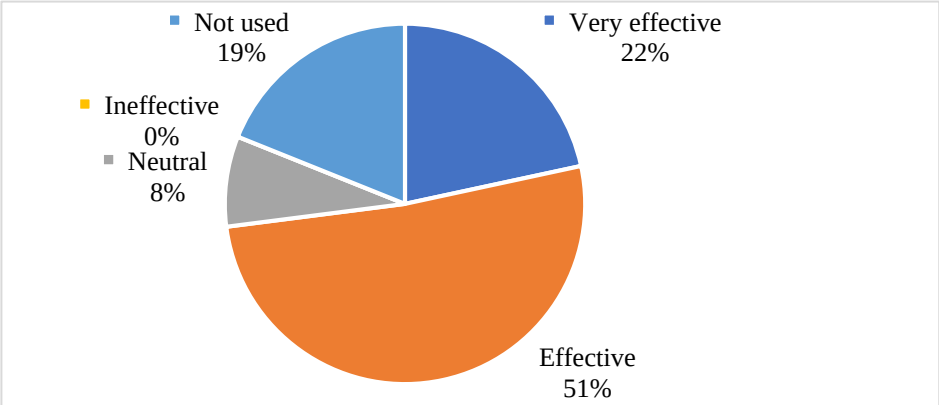



**Source**: BIBM Survey

### 4.5 Effectiveness of AI at Identifying and Classifying Cybersecurity Assets and Risks

In Figure-5, the data reveal a strong and widespread affirmation of AI's utility in the foundational task of asset and risk identification. A significant majority of the banks, totalling 73 percent, expressed positive sentiment regarding AI's performance. This area represents a mature and reliable entry point for institutions beginning their AI journey in cybersecurity. This is composed of a substantial 51 percent who rated its effectiveness as 'Effective' and an additional 22 percent who considered it 'Very effective'. Critically, not a single respondent found AI to be ineffective, underscoring its reliability in this domain. However, the data also shows that adoption is not yet universal, as 19 percent of banks reported they have 'Not used' this technology for asset management, signifying a remaining segment of the industry that has yet to leverage these capabilities.

**Figure-05: Effectiveness of AI at Identifying and Classifying Cybersecurity Assets and Risks**

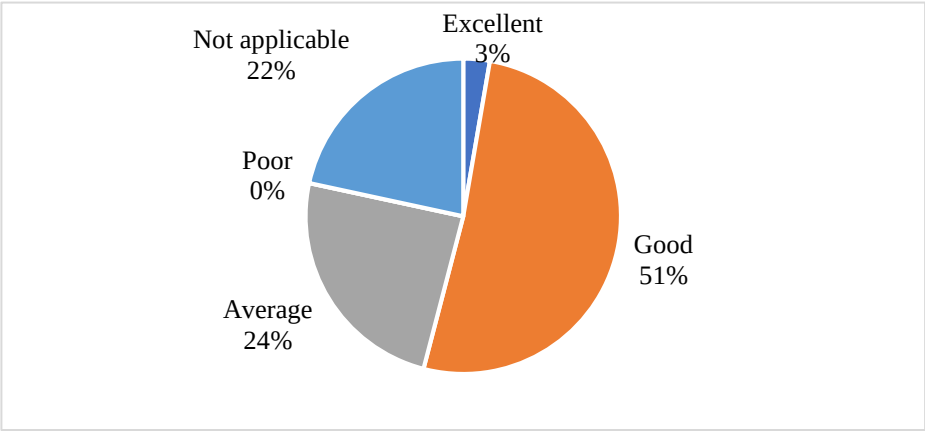



**Source**: BIBM Survey

### 4.6 Effectiveness of AI Tools at Reducing False Positives in Cybersecurity Alerts

Figure-6 indicates that AI is a valuable and widely appreciated tool for managing the persistent challenge of false positive alerts. Over half of the respondents (51%) described their AI tools' performance as 'Good', suggesting a consistent and noticeable improvement in alert reliability. A further 24 percent rated the effectiveness as 'Average', implying a functional but less transformative impact. While only a small fraction (3%) deemed the performance 'Excellent', it is highly significant that no institution reported a 'Poor' outcome. This demonstrates that while the technology may not have perfected the task, it consistently provides a positive contribution. A substantial 22% of respondents classified this question as 'Not applicable', indicating that a considerable portion of the sector does not yet use AI specifically for this purpose.

**Figure-06: Effectiveness of AI Tools at Reducing False Positives in Cybersecurity Alerts**

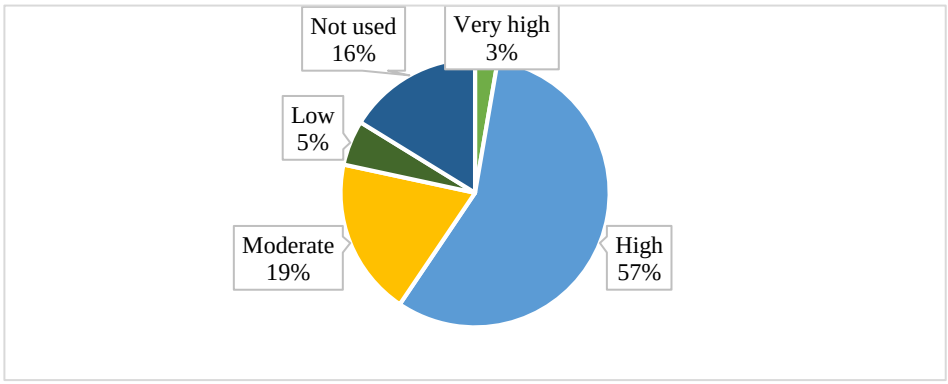



**Source**: BIBM Survey

### 4.7 Effectiveness of AI at Strengthening Protection (e.g., Encryption, Endpoint Security)

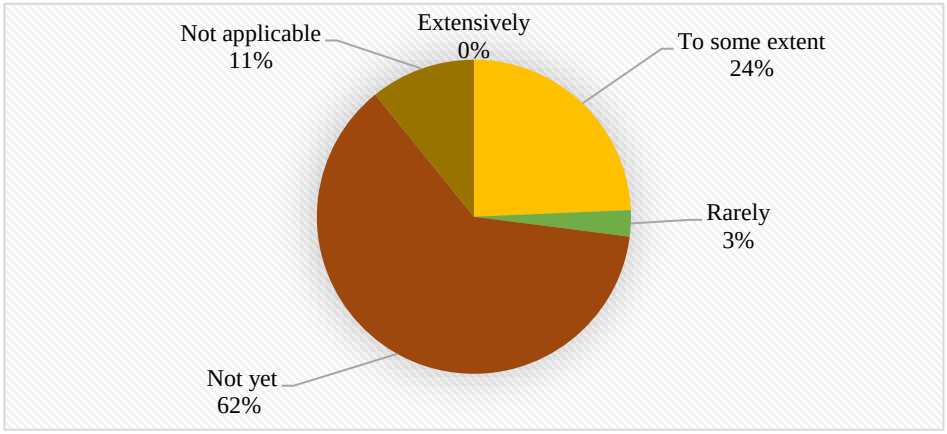
In Figure-7, the data reveals a very high level of confidence in AI's role in strengthening proactive cybersecurity defences. A commanding majority, totalling 60 percent, gave AI a high-performance rating, comprising 57 percent who found its effectiveness to be 'High' and 3 percent who rated it as 'Very high'. This strong endorsement suggests that AI-powered tools are delivering tangible results in preventing security breaches at the network edge and on endpoints. A smaller cohort of 19 percent perceived a 'Moderate' impact, while only 5 percent saw a 'Low' effectiveness. This indicates that negative experiences are rare. Similar to other areas, 16 percent of banks reported they have 'Not used' AI for this function, highlighting an opportunity for broader adoption.

**Figure-07: Effectiveness of AI At Strengthening Protection (e.g., Encryption, Endpoint Security)**




**Source**: BIBM Survey

**Figure-08: AI to Automate Access Control and Authentication**




**Source**: BIBM Survey

### 4.8 AI to Automate Access Control and Authentication

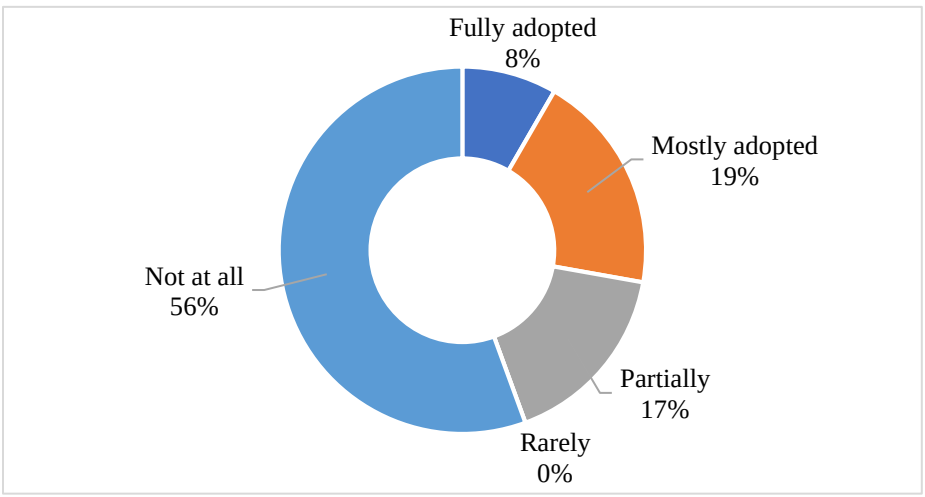
The results of the survey clearly show that the use of AI in the banking industry of Bangladesh to automate access control and authentication is still in an early and exploratory phase. In Figure-8, a striking 62 percent (a significant majority) of banks reported that they have 'Not yet' begun to implement AI for these critical functions. Of the small fraction that has

started, 24 percent are using it only 'To some extent'. The extremely low figure of 3 percent using it 'Rarely' and a complete absence of any bank using it 'Extensively' (0%) paints a picture of extreme caution. This indicates a widespread reluctance to delegate control over user identity and access permissions to automated systems. So, this highlights a major gap between AI's potential and its current application in Access Management.

### 4.9 Applying the Principle of Least Privilege (PLP) for AI-enabled Cybersecurity Data Access

Figure-9 uncovers a deeply concerning gap in cybersecurity governance related to AI implementation. A clear majority of respondents, 54 percent, openly admitted that they do 'Not at all' apply the Principle of Least Privilege (PLP) for their AI systems' data access. This finding suggests that more than half of the AI tools in the sector are operating with excessive permissions, a fundamental concern of security best practices. Conversely, a mere 8 percent have 'Fully adopted' PLP, with another 19 percent having 'Mostly adopted' it. This stark imbalance highlights a systemic failure to apply basic security hygiene to new and powerful technologies.

**Figure-09: Principle of Least Privilege (PLP) for AI-enabled Cybersecurity Data Access**

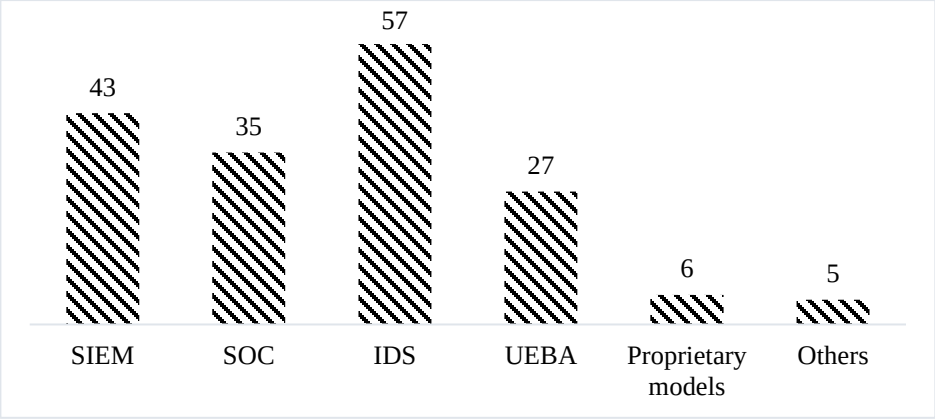



**Source**: BIBM Survey

### 4.10 AI-powered Tools Used for Anomaly Detection in Cybersecurity

There is high adoption of traditional, perimeter-focused tools like Intrusion Detection Systems (IDS) (57%) and Security Information and Event Management (SIEM) (43%). This indicates the banks prioritize basic network defence, centralized log management, and regulatory compliance. Adoption drops sharply for advanced tools like User and Entity Behavior Analytics (UEBA) (27%). UEBA is critical for detecting subtle insider threats and compromised accounts. Its low rate suggests challenges related to data quality, legacy systems, and a shortage of advanced AI/ML expertise.

**Figure-10: AI-powered Tools Used for Anomaly Detection in Cybersecurity**



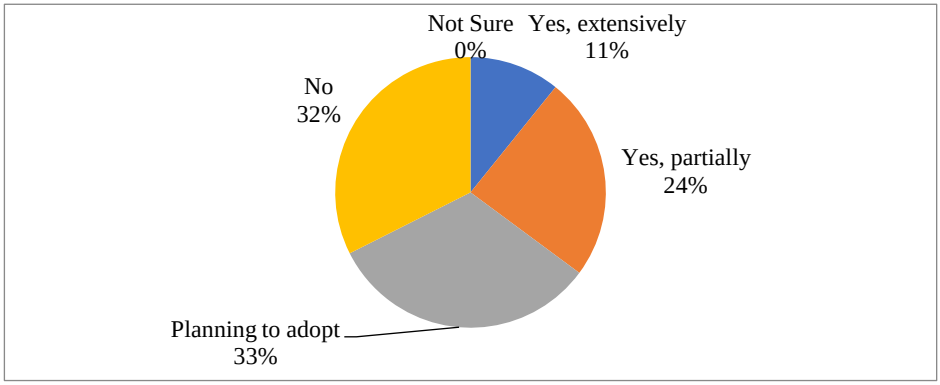

**Source**: BIBM Survey

### 4.11 Security Information and Event Management (SIEM) System Uses AI for Real-time Analysis of Security Alerts

The survey findings reveal that AI adoption in Security Information and Event Management (SIEM) systems among Bangladeshi banks is at an emerging stage. Among the participating banks, 11 percent reported using AI extensively and 24 percent partially, indicating that about one-third have already integrated AI into their cybersecurity monitoring processes. Additionally, 33 percent of banks are planning to adopt AI-based SIEM solutions, reflecting strong future interest and awareness of AI's potential in enhancing real-time threat detection. However, an equal proportion

(32%) has not yet implemented AI, suggesting barriers such as cost, technical expertise, or organizational readiness. Notably, none of the respondents were uncertain about their AI usage status, which highlights a clear understanding of technological adoption levels across the sector.

**Figure-11: SIEM System Uses AI for Real-time Analysis of Security Alerts**




**Source**: BIBM Survey

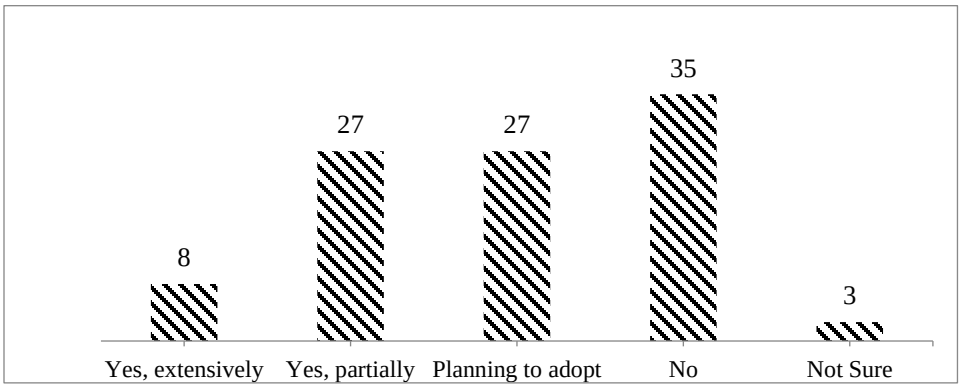
### 4.12 Security Operations Center (SOC) Uses AI for Threat Correlation and Incident Prioritization in Cybersecurity

The survey sought to determine whether the Security Operations Centers (SOC) of Bangladeshi banks utilize Artificial Intelligence (AI) for threat correlation and incident prioritization in cybersecurity management. Among the respondent banks, 8 percent reported using AI extensively, while 27 percent indicated partial adoption. This means that approximately 35 percent of banks have already incorporated AI-based functionalities into their SOC operations to some extent. Additionally, 27 percent of banks are planning to adopt AI in the near future, showing a positive trend toward integrating intelligent automation in threat detection and response processes. However, 35 percent of the banks reported not using AI in their SOCs, while 3 percent remained uncertain about their current adoption status.

Further responses from the banks that have implemented AI revealed several tools in use, such as Playbook design**,** Malware Analysis systems**,** NetWitness SIEM**,** IBM QRadar**,** and Dark Web Monitoring and Honeypot

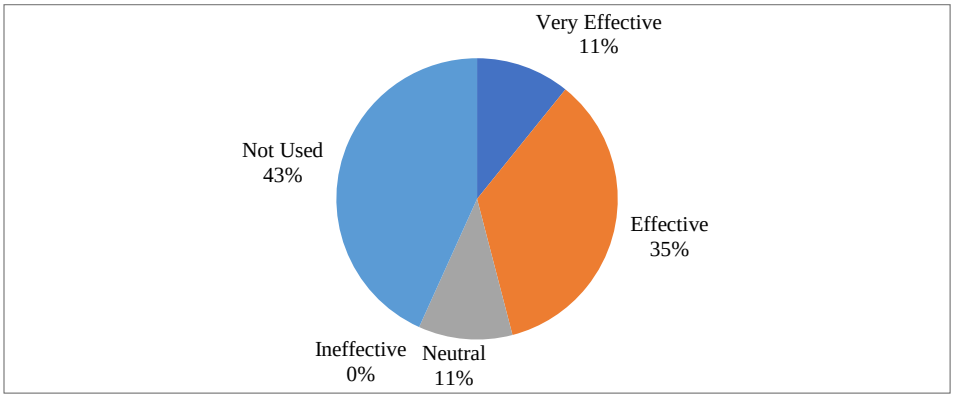
mechanisms. These indicate that some banks are leveraging advanced AI-powered platforms for behavioral analytics, automated threat detection, and real-time incident response.

**Figure-12: SOC uses AI for Threat Correlation and Incident Prioritization in Cybersecurity**




**Source**: BIBM Survey

**Figure-13: AI-powered Intrusion Detection Systems (IDS) Integrated into the Bank's Cybersecurity Monitoring**




**Source**: BIBM Survey

### 4.13 AI-powered Intrusion Detection Systems (IDS) Integrated into the Bank's Cybersecurity Monitoring

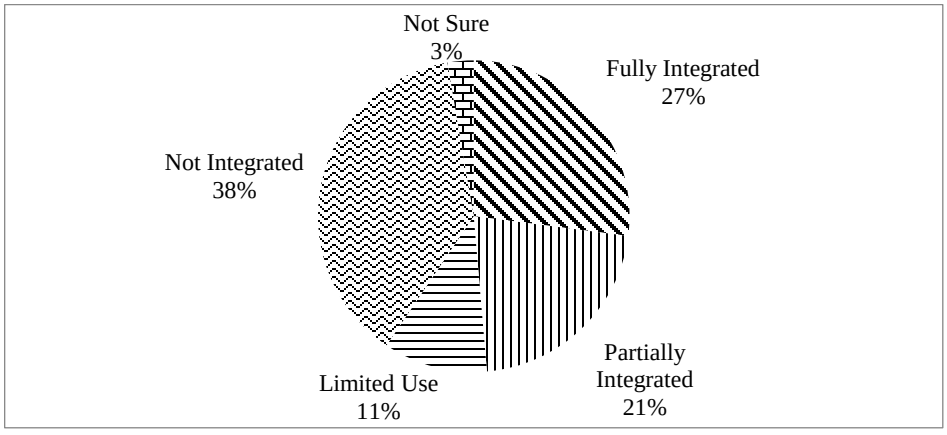
The survey findings indicate that the integration of AI-powered Intrusion Detection Systems (IDS) among the surveyed banks in Bangladesh remains at an early stage, with 43 percent of institutions reporting that they do not

currently utilize this technology. However, among the banks that have adopted AI-powered IDS, the feedback is overwhelmingly positive: 46 percent of the total sample rated the systems as Effective (35%) or Very Effective (11%). This disparity highlights a significant potential for future adoption, with current users implementing either custom AI/ML frameworks (like Deep Learning and Neural Networks) or integrated solutions.

### 4.14 Integration of AI with Intrusion Prevention Systems (IPS) for Real-time Cybersecurity Response

This survey question assesses the integration level of AI with Intrusion Prevention Systems (IPS) for real-time cybersecurity response across the surveyed banks. The data reveals that while a significant portion of banks are actively using AI for prevention, a plurality has yet to integrate it. Specifically, 27 percent of banks report being Fully Integrated, and another 21 percent are Partially Integrated, meaning that almost half (48%) of the sector is actively leveraging AI for automated, real-time threat response. However, the largest single group is the Not Integrated segment, accounting for 38 percent of banks, which, when combined with the Limited Use (11%) and Not Sure (3%) categories, shows that the majority of banks are either not using or are minimally using AI for IPS. Banks are employing both in-house methodologies, such as Deep Learning, Neural Networks, and various Machine Learning techniques and commercial vendor solutions.

**Figure-14: Integration of AI with IPS for Real-time Cybersecurity Response**



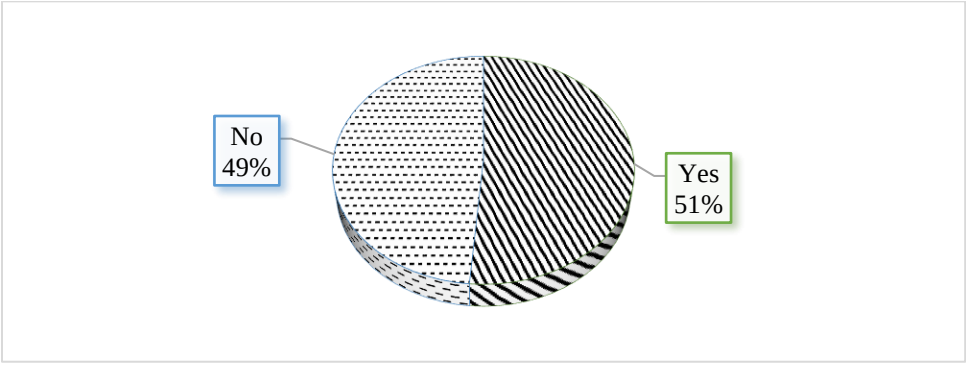

**Source**: BIBM Survey

### 4.15 AI for Phishing Detection

The data reveal a stark division within the Bangladeshi banking sector regarding the use of AI to combat phishing attacks. As per Figure-15, the adoption rate is almost perfectly split, with a slight majority of 51 percent confirming that they do use AI to analyze email content and metadata to identify phishing attempts. However, a very substantial minority of 49 percent reported that they do not use phishing, which is consistently one of the most significant and damaging attack vectors for the financial industry. This nearly 50/50 split is a major point of concern.

It highlights a critical divergence in security maturity. Half of the sector not leveraging AI is likely more vulnerable to modern, evasive phishing campaigns that are specifically designed to bypass legacy security filters. This presents a clear and urgent opportunity for nearly half the industry to significantly upgrade a crucial defence layer and better protect their customers and assets.

**Figure-15: AI for Phishing Detection**



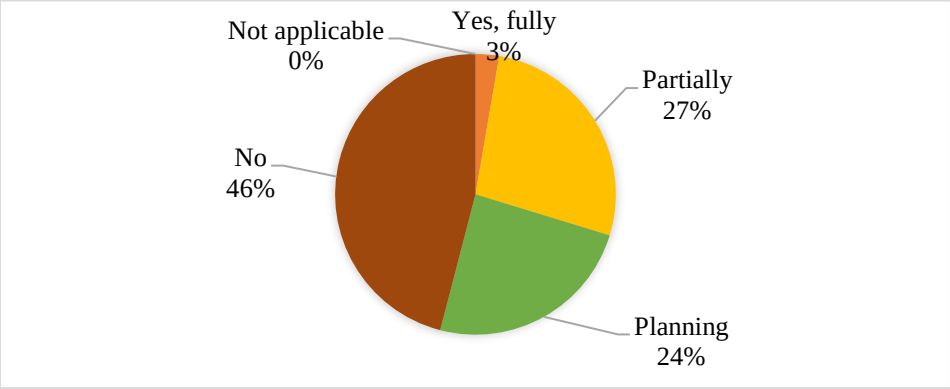

**Source**: BIBM Survey

### 4.16 Use of AI to Automate Incident Response in Cybersecurity

The findings clearly indicate that the use of AI to automate incident response actions is an area of low maturity and high caution. In Figure-16, a variety of banks, 46 percent, reported having 'No' automation in place whatsoever. A further 24 percent are only in the 'Planning' phase, suggesting that actual implementation has not yet begun. Of the banks that have started,

27 percent have achieved 'Partial' automation, likely focusing on simple, repetitive tasks. A negligible 3 percent claimed to have a 'fully' automated incident response system, making this an extreme

**Figure-16: Use of AI to Automate Incident Response in Cybersecurity**

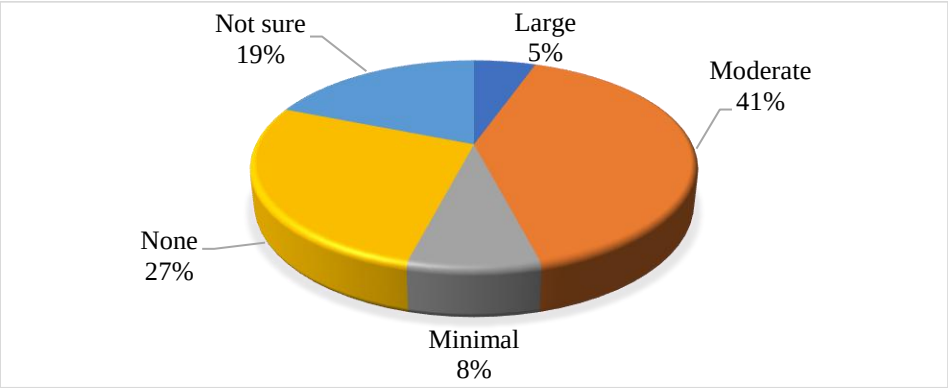



**Source**: BIBM Survey

### 4.17 AI in Post-Incident Cybersecurity Analysis

The perceived benefit of AI in the crucial phase of post-incident analysis and digital forensics is decidedly mixed. In Figure-17, the most common response was 'Moderate', cited by 41 percent of participants, suggesting that AI provides some value but is not a transformative solution for most. However, a significant combined group of 35 percent reported that AI provides either 'None' (27%) or 'Minimal' (8%) help. Furthermore, 19 percent were 'Not sure' of its impact. Only a very small minority of 5 percent felt that AI's contribution to post-incident analysis was 'Large'. The large number of "None," "Minimal," and "Not sure" responses strongly suggests a potential gap in either the AI tools' analytical capabilities or the security analysts' training on how to properly leverage them for deep forensic investigation.

**Figure-17: AI in Post-Incident Cybersecurity Analysis**

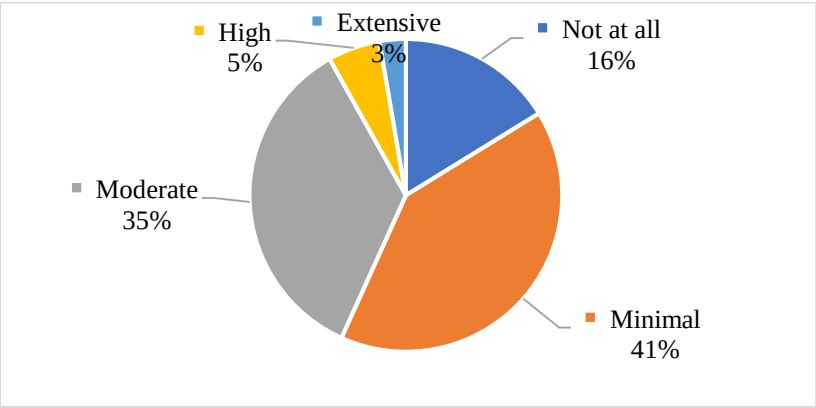



**Source**: BIBM Survey

### 4.18 Level of AI adoption in banks for Fraud Detection, Anomaly Detection, and Threat Intelligence

The pie chart shows the level of AI adoption in banks for key cybersecurity applications, namely fraud detection, anomaly detection, and threat intelligence. The data reveal that AI implementation in these areas remains relatively limited across most banks. A substantial 41 percent of respondents reported minimal adoption, while another 35 percent indicated a moderate level of implementation. This suggests that although banks are aware of AI's potential in strengthening cybersecurity, many are still in the early or experimental stages of deployment. Only 5 percent of banks reported a high level of AI adoption, and a mere 3 percent indicated extensive use. Meanwhile, 16% of respondents stated no adoption at all, indicating that a considerable number of respondent banks have yet to embrace AI in their security frameworks.

**Figure-18: AI adoption in Banks for Fraud Detection, Anomaly Detection, and Threat Intelligence**

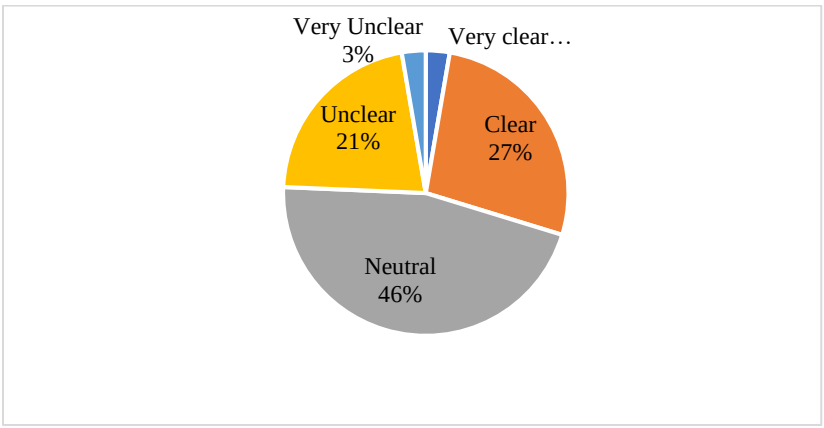



**Source**: BIBM Survey

### 4.19 Clarity of Regulatory Frameworks on AI and Cybersecurity in Bangladesh

The pie chart illustrates respondents' perceptions of how clear the current regulatory frameworks on Artificial Intelligence (AI) and cybersecurity are in Bangladesh. The largest portion of respondents, 46%, identified their view as neutral, suggesting that banks find them ambiguous in application. Meanwhile, 27 percent of respondents considered the frameworks to be clear. On the other hand, 21% viewed the regulations as unclear, and an additional 3 percent found them very unclear. Only 3 percent rated the frameworks as very clear.

**Figure-19: Clarity of Regulatory Frameworks on AI and Cybersecurity in Bangladesh**

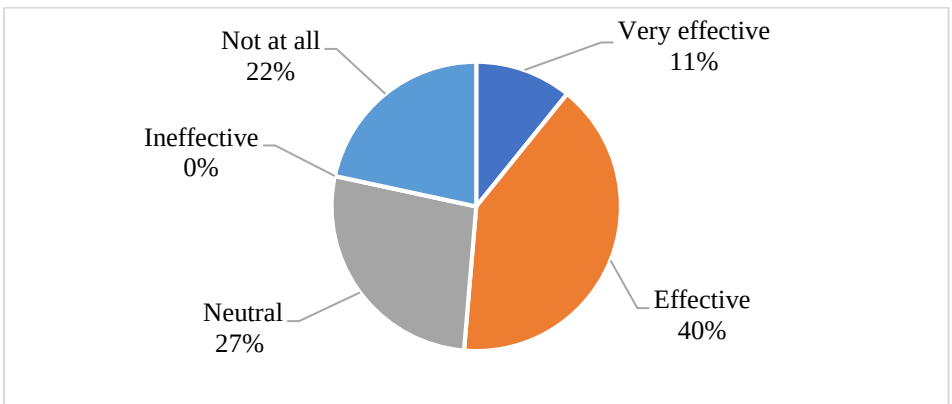



**Source**: BIBM Survey

### 4.20 Collaboration between Banks and Regulators on AI Implementation in Cybersecurity

The survey results reveal nuanced perceptions regarding the collaboration between banks and regulators on AI implementation in cybersecurity. A combined 51 percent of respondents rated their bank's collaboration as either "effective" (40%) or "very effective" (11%), suggesting that more than half of the participants acknowledge positive cooperative efforts. However, a notable 27 percent adopted a "neutral" standpoint, indicating ambivalence or lack of substantial experience with such collaborations. Strikingly, while none rated the collaboration as "ineffective," a significant 22 percent selected "not at all," highlighting a portion of the sample who perceive an absence of effective cooperation in this domain.

**Figure-20: Collaboration between banks and Regulators on AI Implementation in Cybersecurity**




**Source**: BIBM Survey

### 4.21 Implementation of Any Internally Developed AI Tools to Detect and Prevent Anomalies

Banks should have in-house skilled professionals to develop AI tools internally to detect anomalies and enhance the capacity of cybersecurity risk management. However, the study finds that only 8% of banks have implemented internally developed AI tools.

### 4.22 Current Status of Undertaking Training and Capacity-Building Initiatives

Training Programs or Capacity Building initiatives play an important role in developing skilled manpower capable of efficiently managing AI-driven banking and cybersecurity operations. Bank management should give proper insights and allocate sufficient budget for providing adequate, effective training in the area of AI-driven business and associated cyber risk management. But, according to the study (Table-02), we observe a very weak scenario in providing the necessary training for AI-based skill development.

**Table-02: Current Status of Training and Capacity-Building Initiatives Undertaken between 2022 and 2025**

| Area of Training and Capacity-Building Initiatives Undertaken | Total No. of Employees (of 38 Responding Banks) [Participated in Training Programs] | | | |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | 2025 (Jan to Sep) |
| AI-based Banking Operations | 34 | 41 | 198 | 180 |
| AI-based Cybersecurity Management | 21 | 30 | 32 | 44 |

**Source**: BIBM Survey

### 4.23 List of Training Programs, Workshops, Or Capacity-Building Initiatives for Bank Officials

The following table (Table-04) depicts the names or titles of training programs, workshops, seminars, or capacity-building initiatives taken by the banks for their officials with a view to enhancing their skills in AI-driven banking and cybersecurity management between 2022 and 2025 (Jan to Sep). It is notable that only 20% of banks provide data in this regard, which indicates that 80% of banks do not take any initiatives for giving AI-based training. Another important issue is that most of the courses mentioned in

Table-03, are not at an advanced level with sufficient duration to ensure the AI skill development.

**Table-03: The Names or Titles of Training Programs, Workshops, or Capacity-Building Initiatives**

| SL No. | Names or Titles of Training Workshops, or Capacity-Building Initiatives | Year |
|---|---|---|
| 1 | ABB Cybersecurity Summit 2022 | **2022** |
| 2 | Banking Technology and Cyber Securities Issues | |
| 3 | Sandboxing in Cybersecurity | |
| 4 | Training on Email Security Solution | |
| 5 | Kaspersky Endpoint Security and Management (including EDR) | |
| 6 | Advanced Malware Analysis and Ransomware Attack and Investigation | |
| 7 | Cybersecurity and Fraud Prevention in Banks' IT Officials | **2023** |
| 8 | Fin Tech, Reg Tech, and Blockchain Technology in Banks | |
| 9 | Security Operations Center (SOC) in Banks | |
| 10 | Cloud Expo ASIA and Cybersecurity World | |
| 11 | Threat Intelligence Analyst (CTIA) | |
| 12 | Open-Source Intelligence (OSINT) | |
| 13 | Training on Artificial Intelligence | **2024** |
| 14 | Guidelines on ICT Security for Banks and FIs | |
| 15 | Fin Tech, Reg Tech, and Blockchain Technology in Banks | |
| 16 | IT Security and Fraud Prevention in Banks for Business Officials | |
| 17 | Artificial Intelligence (AI) in Banking | |
| 18 | Seminar on "Stakeholders' Readiness for AI-Driven Banking Business in Bangladesh." | |
| 19 | Cybersecurity Conference | **2025 (Jan to Sep)** |
| 20 | Fin Tech, Reg Tech, and Blockchain Technology in Banks | |
| 21 | Artificial Intelligence (AI) in Banking | |

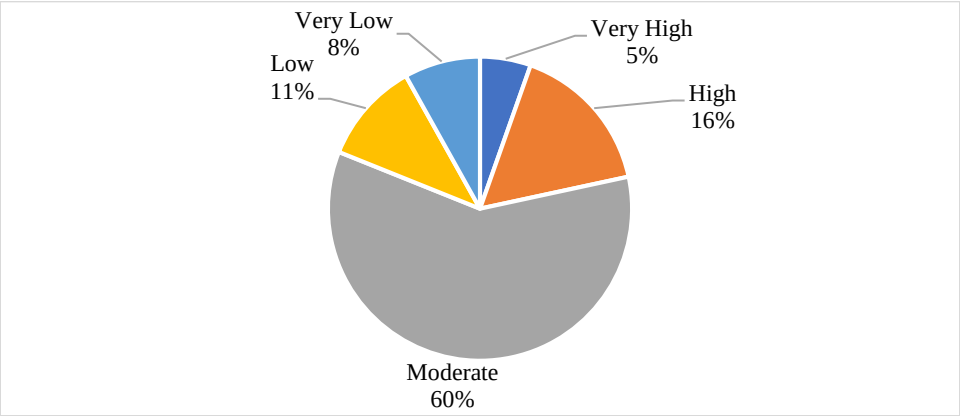
| SL No. | Names or Titles of Training Workshops, or Capacity-Building Initiatives | Year |
|---|---|---|
| 22 | Course on Certified SOC Analyst (CSA) | |
| 23 | Firewall Essentials: Configuration and Management 2025 | |
| 24 | Understanding the Role of Users and Admins of PAM 2025 | |
| 25 | Al in Banking and NBFI- Smart Tools for Smarter Banking | |

**Source**: BIBM Survey

### 4.24 Plan to Allocate IT Budget for AI in Cybersecurity

The data shows that a majority of banks (60%) plan to allocate a moderate portion of their IT budget for AI in cybersecurity. A smaller segment, about 21 percent of banks, is allocating a high or very high budget, indicating strong commitment and prioritization of AI-driven cybersecurity initiatives. Conversely, roughly 19 percent of banks plan for a low or very low allocation, suggesting limited focus or resource constraints in adopting AI for cybersecurity. Overall, most banks recognize AI as an important tool, but the level of financial commitment varies significantly, reflecting differing strategic priorities and maturity levels in AI adoption.

**Figure-21: Plan to Allocate IT Budget for AI in Cybersecurity**

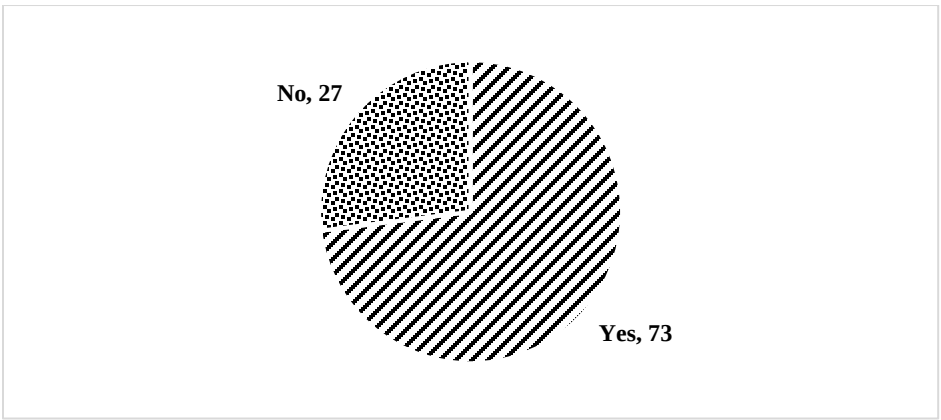



**Source**: BIBM Survey

### 4.25 Board of Directors (BoDs) or Senior Executive Management Formally Discussed the Adoption of AI in Cybersecurity Management

The pie chart illustrates the extent to which banks' Boards of Directors (BoDs) or Senior Executive Management have formally discussed the adoption of Artificial Intelligence (AI) in cybersecurity management. A substantial majority of respondents (73%) indicated *"Yes"*, suggesting that strategic-level engagement with AI-driven cybersecurity initiatives has become a mainstream governance concern in the banking sector. This high percentage implies growing recognition among top management of the importance of integrating AI to strengthen cyber resilience, enhance threat detection, and reduce operational vulnerabilities. Conversely, 27 percent of respondents answered "No", indicating that a notable minority of banks have yet to initiate formal board-level deliberations on AI in cybersecurity. This gap may reflect disparities in organizational maturity, risk appetite, or resource capacity, particularly among smaller or less digitally advanced institutions.

**Figure-22: Board of Directors (BoDs) or Senior Executive Management Formally Discussed the Adoption of AI in Cybersecurity Management**



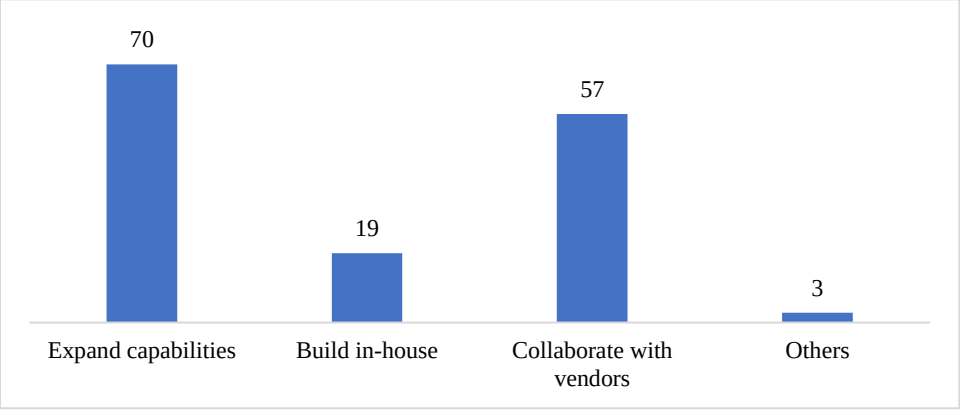

**Source**: BIBM Survey

### 4.26 Bank's Future Plans for AI Adoption in Cybersecurity

The data indicates that a significant majority (70%) of banks plan to expand AI capabilities in cybersecurity, highlighting strong strategic intent to leverage AI for enhanced threat detection, response, and overall cyber resilience. Around 57 percent of banks aim to collaborate with vendors,

showing a preference for partnerships and external expertise to accelerate AI adoption. Meanwhile, 19 percent of banks plan to build AI capabilities in-house, suggesting a focus on developing proprietary solutions and retaining full control over AI systems.

**Figure-23: Bank's Future Plans for AI Adoption in Cybersecurity**

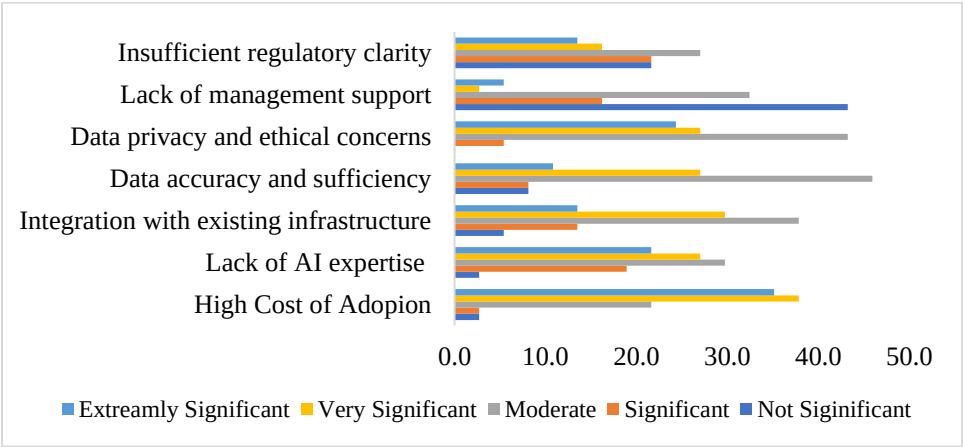



**Source**: BIBM Survey

### 4.27 Challenges Banks Face in Adopting AI for Cybersecurity

The survey data from banks reveals that the "High Cost of Adoption" is perceived as either "Very Significant" (38%) or "Extremely Significant" (35%) by the vast majority, highlighting financial barriers as a crucial concern in implementing AI for cybersecurity. Similarly, "Data privacy and ethical concerns" are seen as "Very Significant" (27%) or "Extremely Significant" (24%) by over half of the respondents, while "Lack of AI expertise" also scores high, with 27 percent rating it as "Very Significant" and 21 percent as "Extremely Significant". In contrast, "Lack of management support" is mostly regarded as "Not Significant" (43%), suggesting that executive buy-in is less of an impediment compared to technical, regulatory, and financial obstacles.

**Figure-24: Challenges Banks Face in Adopting AI for Cybersecurity**




**Source**: BIBM Survey

### 4.28 Summary of Bank Executives' Views on AI Integration in Cybersecurity Management

The following table summarizes the comments or suggestions of bank executives regarding the use of AI in Cybersecurity or AI integration with Cybersecurity Management in Banks.

**Table-04: Bank Executives' Views on AI Integration in Cybersecurity Management**

| SL | Thematic Area | Summarized Insights / Key Findings |
|---|---|---|
| 1. | Strategic Role of AI | Banks view AI as a transformative enabler for strengthening cybersecurity through real-time threat detection, fraud prevention, automation, and predictive analytics. AI is essential for combating increasingly sophisticated, AI-driven cyber threats. |
| 2. | Operational Benefits | AI enhances efficiency, compliance, and cost-effectiveness by automating security operations, supporting continuous monitoring, and improving incident response capabilities. |
| 3. | Implementation Enablers | Successful AI integration depends on data quality, skilled workforce, adequate budget, staff training, and continuous model improvement. The need for AI-specific skill development and integration with legacy systems was emphasized. |
| 4. | Governance and Data Management | Banks stressed the importance of strong data governance, explainable AI (XAI), and transparency in |

| SL | Thematic Area | Summarized Insights / Key Findings |
|---|---|---|
| | | AI-based decision-making to ensure accountability, audit readiness, and regulatory trust. |
| 5. | Challenges and Risks | Common challenges include high implementation cost, shortage of expertise, algorithmic bias, false positives, lack of explainability, and regulatory uncertainty. Banks highlighted the need to manage adversarial AI risks and maintain human oversight in decision-making. |
| 6. | Regulatory Expectations | Most banks urged Bangladesh Bank to issue clear and comprehensive guidelines on AI ethics, data sharing, privacy, risk management, and compliance for uniform adoption across the sector. |
| 7. | Human and Organizational Readiness | Respondents emphasized AI as an augmentation, not a replacement of human expertise. Continuous training, upskilling, and workforce readiness are essential for effective AI-driven cybersecurity operations. |
| 8. | Institutional Initiatives | A few banks have taken proactive measures, such as establishing dedicated AI units under digital banking divisions to promote AI-based innovation and readiness. |
| 9. | Future Outlook | The overall sentiment reflects a cautious confidence that AI is being seen as a key pillar of next-generation cyber defense, provided it is deployed responsibly, transparently, and in compliance with regulatory standards. |

**Source**: BIBM Survey

## 5. Recommendations

### 5.1 Enterprise-Wide AI Governance and Policy Framework

Banks may prioritize establishing a comprehensive policy that defines the scope, objectives, and governance of AI initiatives. This may include ethical AI principles, risk management, and regulatory compliance. Additionally, banks may work on establishing an AI steering committee or governance body responsible for oversight, monitoring, and evaluation of AI projects.

### 5.2 Dedicated AI Cybersecurity Policy and Ethical Safeguards

Absence of formal policies in most banks could imply potential risks related to inconsistent AI implementation, regulatory non-compliance, and challenges in aligning AI-driven security measures with organizational objectives. Banks may prioritize the development of comprehensive AI

adoption policies for cybersecurity to ensure consistent, secure, and compliant use of AI technologies. The rapidly evolving cyber threat landscape is compelling banks to rethink traditional defence mechanisms and increasingly rely on AI for proactive threat management. It is also important to examine the implications of using AI for operational efficiency, including its impact on human oversight, automation, and potential cost-benefit trade-offs. Another crucial issue is customer protection, particularly how AI systems can balance data security and privacy without compromising user trust. Banks should focus on addressing ethical and strategic challenges, such as transparency, accountability, and bias in AI decision-making, as the sector becomes more dependent on machine intelligence for cybersecurity defence.

### 5.3 Holistic AI Deployment Across Detection, Prevention, and Governance

Banks may prioritize AI implementation in dynamic and threat-intensive areas, particularly those requiring real-time decision-making and adaptive learning. However, strategic underinvestment in administrative and preventive functions, such as policy automation and identity management, highlights a gap that could limit long-term resilience. Banks may expand AI use beyond detection to include prevention, governance, and predictive modelling, which will be crucial for developing a holistic AI-driven cybersecurity ecosystem within the banking sector.

### 5.4 AI-Driven Endpoint and Encryption Enhancement Strategy

AI's ability to detect subtle anomalies and zero-day threats on endpoints provides a tangible improvement over traditional signature-based security. This high perceived effectiveness is a key driver for investment and is likely to encourage deeper integration of AI into the primary defence layers of banking cybersecurity architecture.

### 5.5 Transition from IDS/SIEM to AI-Based UEBA Architecture

Banking sector's AI adaptation in cybersecurity is currently focused on detection (IDS/SIEM) rather than proactive behaviour analysis (UEBA). This indicates that while the industry is compliant with baseline security

measures, it remains vulnerable to the more sophisticated, hard-to-detect threats originating from internal access or compromised credentials. Banks can adopt AI-powered tools for anomaly detection in cybersecurity.

### 5.6 Accelerating AI-Driven SOC in Bangladeshi Banks

A moderate but growing adoption of AI within SOCs across Bangladeshi banks. While a significant number of institutions are either using or planning to use AI-driven solutions, a comparable portion of banks still rely on conventional or semi-automated systems. This pattern suggests that although awareness and readiness for AI integration are increasing, barriers such as high costs, technical complexity, and shortage of skilled cybersecurity professionals may be slowing widespread implementation. Nonetheless, the results reflect a progressive movement toward intelligent and automated SOC frameworks in Bangladesh's banking sector, aligning with global cybersecurity transformation trends. Banks/FIs ought to formulate strategies that are short-term, medium-term, and long-term to address financial, technical, and human resource obstacles in expediting the incorporation of AI-driven Security Operations Centers (SOCs).

### 5.7 Executive-Level AI Cybersecurity Impact Assessment

There is a positive trend toward strategic awareness and governance involvement in AI adoption for cybersecurity, but it also emphasizes the need for broader institutional alignment to ensure that AI implementation is guided by executive oversight, regulatory compliance, and ethical governance frameworks across the entire banking ecosystem. Banks that have not yet engaged in discussions regarding the adoption of artificial intelligence at the executive tier ought to initiate a comprehensive AI Impact and Readiness Assessment that aligns with enterprise risk management and regulatory requirements. This process may include performing a cybersecurity maturity evaluation to pinpoint deficiencies in aspects such as threat detection latency, incident response duration, insider risk surveillance, and fraud analysis. By mapping these vulnerabilities against AI-enabled capabilities such as behavioural analytics, predictive threat intelligence, and automated response mechanisms, banks can quantify

potential reductions in operational risk, financial loss, and compliance exposure. A pilot-based cost–benefit analysis, supported by scenario modeling (e.g., simulated ransomware or credential compromise incidents), can further demonstrate measurable impact. Presenting these findings through a board-level risk dashboard highlighting ROI, risk mitigation potential, regulatory alignment, and governance requirements enables executives to evaluate AI adoption not as a technology experiment, but as a strategic risk management and resilience enhancement initiative.

### 5.8 Strategic AI Cybersecurity Investment Optimization

Banks can ensure that the budget is strategically allocated to AI projects that deliver quantifiable enhancements in cybersecurity, including threat identification, fraud deterrence, and automated incident handling. It is advisable to perform periodic ROI evaluations and capability assessments. They can also perform a cost-benefit analysis to grasp how AI might influence the reduction of cybersecurity risks and operational losses. They also can conduct a cost-benefit analysis to understand the potential impact of AI on reducing cybersecurity risks and operational losses. Even small investments in AI-driven security tools can significantly enhance threat detection and resilience. Finally, they can establish a multi-year AI cybersecurity investment roadmap that aligns with overall IT strategy and regulatory compliance requirements.

### 5.9 Balanced In-House and Vendor AI Development Strategy

Banks that are planning to expand AI capabilities may prioritize initiatives that address critical cybersecurity gaps and ensure proper integration with existing systems and processes. On the other hand, those banks that are planning to collaborate with vendors may establish clear vendor governance frameworks, including data security, compliance, and performance metrics, to maximize benefits and mitigate risks. Finally, those banks that are planning to build in-house AI system may invest in talent development and robust AI governance structures to ensure scalability, reliability, and ethical use of AI. Banks can adopt a hybrid AI capability model.

### 5.10 Cost Reduction and Ethical AI Enablement Framework

The most pressing concern is the high cost of adoption, with the majority of respondents viewing financial barriers as a major impediment to implementation. Data privacy and ethical concerns also emerge as significant challenges, reflecting the need for robust frameworks to ensure responsible use of AI in handling sensitive financial data. Additionally, a lack of AI expertise within the sector underscores the urgency of developing local technical capacity and specialized training programs to support AI-driven cybersecurity initiatives. Interestingly, management support is largely not seen as a major obstacle, suggesting leadership awareness and willingness to embrace AI solutions. Banks should focus on reducing implementation costs, strengthening data governance and ethical standards, enhancing workforce skills, and establishing clear regulatory guidelines to enable secure and effective AI integration in the banking sector.

### 5.11 National AI Cybersecurity Skills Development Initiative

Many banks do not have a well-organized AI training program, and the current initiatives are narrow in focus and inadequate for tackling AI-related cybersecurity issues. This deficiency undermines both institutional preparedness and technical capabilities. The banking industry needs to create a cohesive, multi-level training system that guarantees basic AI-security knowledge as well as advanced expertise.

### 5.12 Improve Data Readiness and Quality of Security Telemetry

Ensuring a bank's security tools and AI models receive complete, consistent, and trustworthy data so that detections are accurate and actionable. Banks should standardize and enhance logs across vital systems such as core banking and payment platforms, IAM/PAM, endpoints, network devices, SWIFT-related systems, cloud services, and essential applications by employing a unified logging schema, synchronized time (NTP), and a well-defined event taxonomy.

## 6. Conclusion

This study examined the adoption of Artificial Intelligence (AI) in cybersecurity management within the banking sector of Bangladesh, revealing that the industry remains at an early yet promising stage of AI integration. While several banks have initiated AI-driven tools primarily in threat detection and monitoring, the overall deployment remains fragmented, limited in scope, and largely concentrated on reactive defence mechanisms rather than predictive and preventive cybersecurity architectures.

However, technological adoption alone is insufficient. The research underscores that strategic leadership commitment is a pivotal factor in accelerating AI integration. An innovative, agile, and risk-aware mindset at the board and executive levels is essential to position AI not merely as a technical upgrade, but as a strategic enabler of enterprise risk management and long-term sustainability. Adequate and strategically allocated budgets must be supported by measurable return-on-investment frameworks and multi-year cybersecurity roadmaps aligned with regulatory compliance and institutional objectives.

Most importantly, the future success of AI in cybersecurity within Bangladesh's banking ecosystem will depend on capacity building and human capital development. Establishing structured training programs, fostering collaboration between banks, regulators, and academic institutions, and developing a skilled pool of AI-security professionals are essential to sustain long-term innovation. Without strengthening local expertise, reliance on external vendors may limit institutional independence and scalability.

In conclusion, the adoption of AI in cybersecurity management in Bangladesh's banking sector represents both a strategic necessity and a transformative opportunity. With proactive governance, sustained investment, regulatory alignment, and comprehensive capacity development, AI can evolve from an emerging tool to a foundational pillar of intelligent, resilient, and future-ready banking cybersecurity in Bangladesh.

# References


Aripin, Z., Saepudin, D., & Yulianty, F. (2024, February). Transformation in the internet of things (iot) market in the banking sector: a case study of technology implementation for service improvement and transaction security. *Journal of Jabar Economic Society Networking Forum*, 1(3), 17-32.

DBS Bank. (2023). Annual Report 2023 – CIO Statement, DBS Bank Limited, Singapore, Refriered from https://www.dbs.com/annualreports/2023/cio-statement.html

DBS Bank. (2023). Artificial Intelligence and Ethics, DBS Bank Limited, Singapore, Retrieved from https://www.dbs.com/artificial-intelligence-machine-learning/artificial-intelligence/artificial-intelligence-balancing-innovation-with-ethics.html

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21, 4759.*

Hernández Aros, L., et al. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. Humanities and Social Sciences Communications, 11, 1130.

Jabbar, H. (2025). AI-Driven phishing detection: Enhancing cybersecurity with reinforcement learning. *cybersecurity,* 5(2), 26.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security,* 24, 119.

Khan, M. S., Islam, M. T., Azad, M. A. K., & Ali, M. (2024). Stakeholders' readiness for AI-driven banking business in Bangladesh. Bangladesh Institute of Bank Management. *Research Monograph 74:* Retrieved from https://www.bibm.org.bd/publications-read.php?id=133

Krishnamurthy, O., & Vemulapalli, G. (2024). Advancing sustainable cybersecurity: Exploring trends and overcoming challenges with generative AI. In *Proceedings* of the International Conference on Sustainable Development through ML, AI, and IoT. 16–25.

LightCastle Partners. (2024). AI in Bangladesh's financial sector. Retrieved from https://www.lightcastlebd.com

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems,* 67, 6969–7055.

Parizad, A., & Hatziadoniu, C. J. (2022). Cyber-attack detection using principal component analysis and noisy clustering algorithms: a collaborative machine learning-based framework. *IEEE Transactions on Smart Grid, 13(6),* 4848–4861. https://doi.org/10.1109/TSG.2022.3176311

Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. (2023*).* Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors,* 23, 2415.

Rahman, K., & Akter, S. (2025). Exploring the role of AI and machine learning in enhancing internet banking adoption in Bangladesh. *Journal of Digital Banking Research,* 4(1), 45–60.

Rjoub, G., et al. (2023). A survey on explainable artificial intelligence for cybersecurity. *IEEE Transactions on Network and Service Management,* 20(4), 5115–5140.

https://digitaldefynd.com/IQ/banking-cybersecurity-case-studies/

# Appendices

## Appendix-I: List of Respondent Banks

| | | | |
|---|---|---|---|
| 1 | Dutch-Bangla Bank PLC | 20 | Trust Bank PLC |
| 2 | One Bank PLC | 21 | Shahjalal Islami Bank PLC |
| 3 | Export Import Bank of Bangladesh PLC | 22 | Premier Bank PLC |
| 4 | Pubali Bank PLC | 23 | IFIC Bank PLC |
| 5 | United Commercial Bank PLC | 24 | Prime Bank PLC |
| 6 | Shimanto Bank PLC | 25 | Al-Arafah Islami Bank PLC |
| 7 | NRB Bank PLC | 26 | AB Bank PLC |
| 8 | Eastern Bank PLC | 27 | Community Bank PLC |
| 9 | First Security Islami Bank PLC | 28 | Mutual Trust Bank PLC |
| 10 | Modhumoti Bank PLC | 29 | Bangladesh Commerce Bank Ltd. |
| 11 | NCC Bank PLC | 30 | Jamuna Bank PLC. |
| 12 | NRBC Bank PLC | 31 | HSBC Bangladesh |
| 13 | Southeast Bank PLC | 32 | Commercial Bank of Ceylon PLC |
| 14 | Union Bank PLC | 33 | Standard Chartered Bank |
| 15 | City Bank PLC | 34 | Janata Bank PLC |
| 16 | Bank Asia PLC | 35 | Sonali Bank PLC. |
| 17 | SBAC Bank PLC | 36 | Agrani Bank PLC. |
| 18 | Midland Bank PLC | 37 | Bangladesh Krishi Bank |
| 19 | Mercantile Bank PLC | 38 | Rajshahi Krishi Unnayan Bank |

## Distribution of Banks

| Banks Category | No of Banks |
|---|---|
| Private Commercial Banks | 30 |
| State-owned Commercial Bank | 3 |
| Specialized Development Bank | 2 |
| Foreign Commercial Bank | 3 |
| **Total** | **38** |

## Appendix-II: Concise Summary of the Related Studies

| Authors & Year | Focus / Application | Methodology / AI Technique | Region / Context | Key Findings |
|---|---|---|---|---|
| Mohamed, 2025 | IDS, malware detection, insider threats, automated response | ML, Deep Learning, CNN, ensemble methods | Global | AI enables proactive threat management, reduces mean time to respond by 70%, and improves anomaly detection against APTs and zero-day attacks. |
| Hernández Aros et al., 2024 | Financial fraud detection | ML models (decision trees, SVM, neural networks) | Global | ML models accurately identify suspicious transactions and detect emerging fraud patterns, improving financial security. |
| Pinto et al., 2023 | Intrusion detection for critical infrastructure | Supervised & unsupervised ML | Global | ML-based IDS enhances real-time detection and response to unusual network behavior, strengthening infrastructure protection. |
| González-Granadillo et al., 2021 | SIEM systems | Deep Learning, event correlation | Global | Deep learning reduces false positives, detects complex threats, and enhances SOC operations for efficient monitoring. |
| Jabbar, 2025 | Phishing detection, document security | NLP, Reinforcement Learning | Global | AI-based NLP detects phishing emails and harmful links before reaching end-users, improving overall cybersecurity. |

| Authors & Year | Focus / Application | Methodology / AI Technique | Region / Context | Key Findings |
|---|---|---|---|---|
| Rjoub et al., 2023 | Explainable AI in cybersecurity | Survey, XAI techniques | Asia | AI adoption extends beyond threat detection to regulatory compliance and reporting, supporting transparency and accountability. |
| Krishnamurthy & Vemulapalli, 2024 | Generative AI-driven threats | Review, case studies | Asia | AI helps banks maintain resilience against emerging AI-driven cyber threats and supports proactive security strategies. |
| Rahman & Akter, 2025 | Internet banking adoption | TAM-based survey | Bangladesh | AI-driven security enhances customer trust in digital banking; perceived security strongly influences adoption decisions. |
| LightCastle Partners, 2024 | AI adoption in financial sector | Industry report | Bangladesh | Banks are experimenting with AI-based fraud detection and chatbots; full-scale integration is limited by cost, legacy systems, and insufficient training data. |
| Khan et al., 2024 | Stakeholder readiness for AI in banking | Survey, research monograph | Bangladesh | Only 6% of banks are fully prepared for AI; key barriers include awareness, infrastructure, budget constraints, and regulatory uncertainty. |

Bangladesh Institute of Bank Management (BIBM)
**Plot No.4, Main Road No. 1 (South), Section No. 2, Mirpur, Dhaka-1216**
**Tel: 48032091-4; 48032097-8, 48032104, E-mail: bibmresearch@bibm.org.bd; Web: www.bibm.org.bd**

**Price: BDT 300.00**
**USD 8.00**