European Journal of Economic and Financial Research
ISSN: 2501-9430
ISSN-L: 2501-9430
Available on-line at: http://www.oapub.org/soc

DOI: 10.46827/ejefr.v8i8.1912 Volume 8 | Issue 8 | 2025

CYBERSECURITY CHALLENGES IN DIGITAL ISLAMIC BANKING ESTABLISHED IN BANGLADESH: RISK MANAGEMENT PERSPECTIVE

Ebrahim Mollik[1i],
Faisal Majeed[2]
[1]MSc,
International Business with Data Analytics,
Ulster University,
United Kingdom
[2]Dr.
Faculty of Business,
Ulster University,
United Kingdom

Abstract:
The rapid expansion of digital banking in impoverished countries presents novel problems, including data security and risk management for the Islamic banking sector. Including digital technologies in Bangladeshi Islamic organizations has made more people able to access services and financial providers. These businesses consequently become more vulnerable to cybersecurity problems such as data breaches, fraud, and cyberattacks, thus jeopardizing customer confidence and the integrity of the financial system. In this study, we investigate how effectively current risk management techniques address the cybersecurity challenges Bangladeshi digital Islamic banking encounters. This study reveals the areas of weakness by comparing global cybersecurity standards and development recommendations with the current systems of well-known Islamic banks in Bangladesh. The article looks at how these problems affect the general application of digital financial services, legislation, and customer confidence. This paper adds to what is previously known about cybersecurity in Islamic banking by providing doable suggestions on how to improve risk management in developing countries. It achieves this through a thorough reading of the body of the present literature, secondary data analysis, and in-depth interviews with important participants. The results clearly suggest that strict cybersecurity rules have to be observed since they complement Islamic financial concepts and the world's best standards. This would ensure that Bangladesh's digital Islamic banking market stays steady and keeps growing.

JEL: G21, G32, K24, L86

[i] Correspondence: email mollikebrahim80@gmail.com

Keywords: cybersecurity in Islamic banking, digital transformation in the banking sector, risk management in banking organizations, Islamic financial theory, monetary frameworks in expanding economies

1. Introduction

1.1 Background and Context

The digital revolution in banking has altered the global financial scene and given poor countries both new opportunities and challenges. The introduction of digital banking services in recent years has made hitherto unthinkable access to financial services feasible, hence increasing client involvement and financial inclusion. Especially in developing nations like Bangladesh, the expansion of digital financial services has created major cybersecurity problems. Maintaining consumer confidence and safeguarding financial transactions depends on keeping the security and integrity of digital platforms, which are becoming ever more crucial as they get included in the banking system.

Bangladeshi Islamic banking has developed dramatically under Shariah law. Islamic banks are increasingly embracing online and mobile banking platforms, notably in underdeveloped rural areas, thanks in great part to their quick acceptance of digital technology to boost their clientele. These developments help to accomplish the aim of financial inclusion, but they also make Islamic financial institutions more susceptible to several cybersecurity concerns, including digital vulnerabilities, data breaches, and cybercrime.

Bangladesh's Islamic banking industry ranks second among all in South Asia, supported by a robust legal framework controlling its activities. Still, the rise of digital banking products presents fresh challenges for customers, financial institutions, and government officials. The challenges include the need for cybersecurity systems that follow Islamic financial ideas and worldwide best standards, as well as improved risk management strategies (Bangladesh Bank, 2024). Bangladesh's Islamic banking sector depends on a strong regulatory framework that closely observes its activities. For customers, businesses, governments, regulatory agencies, and digital banking providers, as well as for financial institutions, the rise of these services does bring new challenges (Asian Bank & Finance, 2023). Among these challenges is the need for improved risk management systems and cybersecurity policies anchored on Islamic finance concepts and the world's best standards. There are several weak cybersecurity policies that could threaten the integrity of the financial system and reduce consumer confidence—a basic feature of Islamic banking, as customer connections rely on trust, and ethical issues are of considerable relevance.

Given the continually changing digital terrain, it is important to evaluate how Bangladeshi Islamic banks handle cybersecurity concerns. Above all, one should be knowledgeable about contemporary risk-reducing strategies, their compliance with Shariah values, and their efficiency (Afrin, 2023). This paper aims to close this disparity

by analysing the cybersecurity problems Bangladeshi digital Islamic banks face and their risk-management techniques.

The findings of this study will add to the academic body of knowledge on digital money, Islamic banking, and developing nation cybersecurity. The article will offer reasonable recommendations for enhancing cybersecurity systems in Islamic banks to ensure security, compliance, and dependability in the face of developing digital threats.

1.2 Problem Statement

Bangladesh's rapid growth in digital banking opens enormous opportunities for client contact and financial inclusion in Islamic banking. Thanks to the digital revolution, Islamic banks today deal with several cybersecurity issues like data breaches, vulnerabilities on online platforms, and criminal activity. Shariah compliance and ethics come first; hence, these challenges jeopardize the integrity and confidentiality of financial transactions, which are vital for maintaining client faith in the Islamic banking system (Bangladesh Bank, 2024).

Digital banking platforms are becoming more and more vital, however, the present cybersecurity policies in Bangladesh's Islamic banking sector are not properly established. Therefore, financial institutions remain vulnerable to cyber-attacks, even if they are becoming more important. Furthermore, even though Bangladesh's regulatory environment in traditional banking has shown incredible development and control, the fast-changing digital landscape presents new problems that need immediate attention and reinforced cybersecurity rules. The lack of a comprehensive risk management strategy that fits Islamic financial concepts aggravates the problem.

This paper aims to reveal their cybersecurity problems and assess the current risk management practices of Bangladeshi digital Islamic banks. The goal is to provide direction for improving cybersecurity policies in compliance with Shariah values, thereby ensuring that Islamic banks maintain their integrity, security, and compliance while managing the complexity of digital change.

1.3 Research Objectives and Questions

1.3.1 Research Objectives

The purpose of this research is to study the realities and challenges of cybersecurity for Islamic banks in digital formats in Bangladesh, as well as recommended countermeasures for optimal risk management.

1) To identify and analyse the different cyber risk factors that digital Islamic banking institutions in Bangladesh experience.
2) To evaluate the strength of the existing cybersecurity policies and risk management strategies adopted by the Islamic banks.
3) To assess the role of Bangladesh Bank and the other regulatory bodies in thus strengthening the cyber security architecture of Islamic financial institutions.
4) To understand the impacts of the cyber security threats on both customers' trust and the financial stability of the Islamic banks.

5) To explore ways of improving system resilience in accordance with Shariah principles.

These objectives will help to better understand the digital security landscape within Islamic banking in Bangladesh and will yield recommendations for strengthening both dimensions of cybersecurity.

1.3.2 Research Questions

The fundamental research question has been tackled as follows:

1) What are the key cybersecurity challenges faced by digital Islamic banking in Bangladesh?
2) What are the effectiveness levels of policies and risk management frameworks in light of current cybersecurity threats in Islamic banks?
3) What is the role of Bangladesh Bank regarding cybersecurity management in the Islamic banking industry?
4) How does cyber threat impact trust and financial stability for customers in the Islamic banking sector of Bangladesh?
5) What cybersecurity mechanisms would further reduce risk within Shariah compliance?

These issues would be dealt with in order to prepare the research for an appropriate analytical framework on the Islamic banking sector for further improvement identification in the entire cybersecurity environment in Bangladesh.

1.4 Significance of the Study

The rapid transition in the banking sector of Bangladesh has made this area quite prone to the occurrence of cyber threats. A study conducted in 2022 by the Bangladesh Institute of Bank Management (BIBM) states that 52% of the banks in Bangladesh are at risk of becoming victims of cyber-process attacks, with about 630 incidents each day. Reports went on to say that among these attacks, 24% were from China, 13% from North Korea, and 12% from Russia (Afrin, 2023).

From the total Tk42,609 crore spent on IT last year, the banks direct 5% of their IT budgets toward securing their systems and a meagre 3% toward training activities. Half of the bank staff are considered not to have a sound knowledge of IT security. Internal IT capability majorly constitutes vulnerabilities, and insufficient cybersecurity measures actually put breaches in place by the vendors and internal personnel (Report, 2022).

BGD e-GOV CIRT revealed that three thousand bank cards of various Bangladeshi banks were found on the dark web, which denotes a liability for the banks of about $43.67 million in irretrievable losses. Core banking systems and Internet Banking gateways were found to be exposed to the Internet without sufficient protection (Afrin, 2023).

Improvement on these issues means that immediate measures must be undertaken to strengthen the cybersecurity of banks and Islamic financial institutions in Bangladesh. An immediate intensification of protective measures, staff training, and strict adherence

to the regulatory framework of the banking sector in countering the rising cyber threat in the digital banking environment would be very important in addressing the threats.

1.5 Brief of Methodology

The study uses secondary data analysis to unearth some vulnerabilities concerning cybersecurity in risk management with respect to the digital Islamic banking paradigm in Bangladesh. The research considers all accredited academic and industrial references to give proper orientation to an analysis of the cybersecurity vulnerabilities of Islamic banking, regulatory impediments, and risk mitigation measures advanced or recommended.

Back-end setting analysis and information gathering provided a backdrop from government regulations and regulatory reports, industry whitepapers, and cybersecurity case studies, the main one being the case of Bangladesh, which is by law the legitimate authority regulating the banking sector and concerning cybersecurity. This is further clarified by reports from the Bangladesh Institute of Bank Management (BIBM) that seem to be highly enlightening regarding the changing cyber realm concerning the banking sector in the country. The additional material has been sourced from the Bangladesh Government Computer Incident Response Team: these deal with any cyber threat and vulnerability concerning financial institutions, certainly including Islamic banks. With a whole lot of reports therein laying precedence for the required statistics, policy background, and archival cyber incidents concerning digital banking operations.

Also, the importance of using some other secondary data sources, such as industrial reports and case studies, cannot be rendered less important. These reports prepared by consultancy firms, cybersecurity companies, and international organizations, including the Financial Stability Board (FSB) and the International Monetary Fund (IMF), would warrant the presentation of a more global view of the cybersecurity framework in whichever banking system. In turn, the case studies of historic breaches in cybersecurity occurring in the country and in Islamic banks will help to better understand the operational risk factors and work with assessing the level of fine-tuning of the enacted risk management strategies.

Again, to maintain academic integrity, a wealth of peer-reviewed journals discussing cybersecurity as a subject matter in Islamic banking, financial risk management, and digital transformation were consulted thoroughly. It is also noted that a firm theoretical basis was espoused and empirical findings or critical discussion on the threats of cybersecurity and risk mitigation strategies were thoroughly reviewed via other reputable databases such as Scopus, ScienceDirect, and Google Scholar. For information on current cyber threats, regulatory responses, and other trends in the cybersecurity landscape of Bangladesh's banking sector, media reports from reputable sources such as The Financial Times, The Daily Star, and The Business Standard were also reviewed.

The thematic approach to the analysis of data thus points to key cybersecurity risks, regulatory challenges, and frameworks for risk management, in addition to

comparative analysis methods that can be employed to juxtapose Bangladesh's measures for cybersecurity in Islamic banking with international best practices. Finally, an analysis of the temporal trends of cyber security incidents reveals possible risks and vulnerabilities attached to such trends.

Having chosen to use secondary data makes sense economically and otherwise, and for a timely setting to address challenges presented by cybersecurity in Islamic banking. Yet it has backed up its macro-assessments, rather with a diverse approach, about the security landscape, the regulatory response, and the readiness of Bangladeshi Islamic banks towards addressing cyber threats admissible by Shariah principles.

2. Literature Review

2.1 Islamic Banking in Bangladesh

Islamic banking has started in this country on a journey and is now gradually climaxing into one of the eminent pillars of the financial system. Such banks have incorporated Shari'ah principles that disallow Riba and advocate risk sharing. Hence, Islamic banks gained great popularity in ethical practice accounting as Islamic formulation with respect to the financial value system of the Muslim majority population in Bangladesh. It came into being as an instrument for the introduction of Islamic banking in the country through IBBL in 1983. The sector did well as more fully fledged Islamic banks began to pour in to add their strata and others with full-blooded conventional banks combined together to create Islamic banking windows (Bank, 2023).

The Bangladesh Bank, as the central monetary authority, had the primary mandate of regularizing and supervising Islamic banking operations. These regulations include Islamic Banking Guidelines handed down by the authority, ensuring that operations are done in the Shariah way, apart from international banking standards. The Central Shariah Board for Islamic Banks of Bangladesh (CSBIB) establishes the standards with regard to Islamic financial integrity in operational banking matters in any jurisprudential issues. The rising digital banking environments have posed natural challenges to the enforcement harmonization of Shariah compliance, particularly risk management and cybersecurity (CSIB, 2020).

Islamic banks contribute adequately towards financial inclusion in Bangladesh, particularly in rural areas, where penetration by conventional banks is minor. The growth of digital banking, for example, MFS, internet banking, etc., allows the public to access banking services without interference with the ethical business mode and profit-sharing avenues of Islamic finance (Hossain, 2022). Nowadays, Islamic banks provide Shariah-compliant digital financial products with organizations such as bKash, Nagad, and Rocket. However, at the same time, the rapid speed of digitization of Islamic banking products also poses new security threats for the sector as breaches of data, fraud, and cyberattacks, which can erode customer confidence and financial stability (Habiba Nowrose, 2024).

It appears that the two most difficult challenges Islamic banking faces at present are liquidity management and standardization of products and processes. While conventional banks enjoy facilities such as interest-based liquidity management, Islamic banks cannot do so because of the non-permissibility of using interest-based instruments, leading to an ever-increasing need for the development of alternative financial means. Moreover, this is greatly limited in managing short-term liquidity by virtue of a well-defined Islamic interbank market and by a limited supply of Sharia-compliant short-term investment products.

At the same time, with the emerging growth of Islamic banking in Bangladesh, the issues of cybersecurity, homogenization of regulatory regimes, and financial innovation will continue to maintain their importance in this regard. Future research and policies should strengthen digital security regimes, bolster regulation, and create and promote Shariah-influenced fintech solutions, all of which will ensure resilience and stability for the Islamic banking sector itself.

2.2 Digital Transforming in Islamic Banking

Digital transformation really disrupted Islamic banking; it brought all innovative technologies, making them fit within Shariah compliance purposes. Mostly in the last 10 years, Islamic banks have aggressively adopted the use of digital finance services such as mobile banking, internet banking, and blockchain-based solutions in order to make services more accessible, efficient, and satisfying for customers. Most of these require financial inclusion, changing customer demands, and global trends toward a digital economy.

Islamic banks do fintech services that provide Shariah-compliant financial products but acknowledge the peculiarities in free-interest banking. These reasons have been in MFS, and the use of e-banking platforms allows clients to perform transactions and apply Islamic financing without having to use regular interest-based methods for investment access. Artificial intelligence and big data analysis have backed up risk management and customized banking experience at the same time well observed in the principles of Islamic finance. They are also exploring the potential applications of the technology known as blockchain to improve further transparency, lower transaction costs, and increase the safeguarding of facilities for transactions in Islamic banking (van de Vann, 2024).

Challenges faced by Islamic banking during the zenith performance in digitalization are formidable ones, particularly in being propelled by a strong force of threats from cybersecurity, regulatory compliance avenues, or standardization concerning digital financial products. Consumer trust and integrity in financial transactions are in peril because of cyber threats such as data breaches, fraud, or ransomware attacks. The very existence of a global standard prevents the creation of a digital Islamic banking framework, thereby changing regulatory frameworks for individual countries and paving the way for differences in implementation in markets (Temenos, 2023).

The contributions of regulatory agencies, including Bangladesh Bank and CSBIB are essential in ensuring digital innovations are in line with Shariah compliance and security protocols. Immediate actions to ensure the continued viability of digital Islamic banking include strengthening cybersecurity frameworks, enhancing risk management strategies, and increasing digital literacy among customers. Going further, intervention should particularly focus on increasing the connecting factors among digital identity verification, cloud computing, and machine learning that can improve trust and security with a more efficient sector.

The opportunities and threats that digital transformation offers to Islamic banking. Innovations using fintech-enabled solutions will deliver greater inclusion with efficiency; however, regulations, cybersecurity, and ethics can be impediments to maintaining trust and security within an increasingly digitized and efficient financial ecosystem.

2.3 Cybersecurity in Banking

The changes in the banking sector are multiplying, fast-tracking the digital transformation for operational efficiency and customer access, accompanied by high risks of exposure to cyber threats. According to a survey conducted by the Bangladesh Institute of Bank Management (BIBM), banks in Bangladesh are at high risk from cyber threats, as 52% of them confront cyber threats with an average of 630 attacks a day. Among these attacks, 24% originate in China, 12% in Russia, and 13% in North Korea (Afrin, 2023).

Islamic Banking works on Shariah principles, and its distinctive operating systems and clients make it more vulnerable to cyber threats. With the advent of digital banking services, they have now become additional loopholes through which cybercriminals can exploit even more anomalies produced by the obsolete traditional banking system. These cybercriminals target banks and try to take advantage of weaknesses in cloud security and manual processes that are prone to human error (Temenos, 2023).

The pullback of the 1-billion-dollar preferable attempt theft of Bangladesh Bank in 2016 was the extant exploitation of the SWIFT payment scheme, thus justly reinforcing considerations with respect to the cybersecurity setting. Had it not been for the blocking of most of these transactions, the magnitude of 81 million dollars in losses would have articulated vulnerabilities lying within the confines of the financial infrastructure (Tim Maurer and Arthur Neloson, 2021).

In line with the statements mentioned above, the central bank has commenced the enforcement of tougher guidelines on cybersecurity for financial institutions. However, compliance by banks remains a patchy affair, the cost being a recurring deterrent to the implementation of some of the measures in the past. Customer-related data matters a lot, and there is a need to maintain utmost confidentiality; proper overall security of financial operations, such as up-to-date audits, advanced training, and investments in top technologies for security, is a must (31st anniversary issue-I, 2025).

As the economy continues to digitize, the growing call for sturdy cybersecurity frameworks in the banking sector is growing in urgency. The banking sector of the

country must tackle these challenges to secure customer assets, maintain faith in the financial system, and seize the upcoming cyber threats when they come.

2.4 Cybersecurity and Challenges in Islamic Banking

Cybersecurity issues are unfolding new. Challenges brought about by digital banking threats to Islamic banks and their clientele abound. Islamic banks, having gone digital for the sake of financial inclusion, given under Islamic Shariah employ the ethics of finance; for example, an interest-based transaction being chiefly forbidden must confront digital transformation instability threats such as phishing, ransomware, and fraudulent activities altogether.

The CIBAFI report holds that the surge in digitalization in Islamic financial services has resulted in an equally large increase in the incidence of cyber risks and attacks against these institutions (CIBAFI, 2021). This report goes on to indicate that owing to the highly lucrative nature of cybercrime, having funds and information available in the financial sector makes this sector target number one for cybercriminals, whereby Islamic banks, in special consideration, are facing odd challenges.

Another great challenge in the attempt to secure Islamic banking operations is the non-existence of an accepted, standardized framework of cybersecurity that has been adapted to suit this Shariah-compliant financial institution. Due to the ageing of IT infrastructure, many Islamic banks today operate with systems that are simply inadequate for addressing highly sophisticated cyber threats. Ethical considerations involved in Islamic finance elevate data protection scrutiny, thus giving data protection precedence with regard to the trust and confidentiality of customers.

Yet, the incident of the cyber heist of the Bangladesh Bank in 2016 exemplifies fractures in the financial sector. The hackers took $101 million by exploiting loopholes in the SWIFT interbank messaging system, with some of the money being laundered via the Philippines' financial channels. Nevertheless, the whole incident-targeting a central bank constantly reminds us of the need-for digital security to be improved in Islamic banks that are adopting mobile and online banking systems (Wikipedia Contributors, 2019).

In this light, some institutions, for example, the BIBM, have taken charge of training managers on aspects of banking and cybersecurity issues. These trainings are aimed at orienting the participants on IT challenges, the role of technology in banking systems, and means of preventing cybercrime and securing banks' information (BIBM, 2021).

There are also several cybersecurity firms that have greatly helped many Islamic banks to reinforce their defences. In Qatar, for example, one Islamic bank enlisted the help of a cybersecurity company to safeguard its data and avert fraud according to Islamic banking requirements. This collaboration has apparently saved over 5,000 potential fraud attempts from the leakage of customer information, thereby proving the effectiveness of a targeted cybersecurity solution (CYBLE, 2024).

2.5 Risk Management Frameworks

Risk management is a fundamental aspect of Islamic banking and involves some equilibrium in financial activity and Shari'ah principles. Interest (riba) and profit-and-loss-sharing being the polar opposite of interest, Islamic banks are tied in a specific way and thus require specialized risk management systems. Other risks affecting Islamic banks are credit risk arising from the other party in the transaction under Mudarabah and Musharakah, market risk arising from the reduced value of the assets, operational risk related to internal processes including Shari'ah compliance, and liquidity risk arising from the mismatch of assets and liabilities. Important aspects are risk identification and Islamic banks' measure possible losses using quantitative tools, thereby stress testing and scenario analysis for extreme events that might have an impact on their financial positioning (Ahmed and Khan, 2007).

Hedging techniques approved by Shari'ah principles, such as profit-rate swaps, are usually applied by Islamic banks to balance such risks with Islamic principles. The collateralization of permissible assets is also practiced covering the financial obligations and containing the default risk. Diversification minimizes concentration risk through the sharing of investments across sectors. Continuous risk monitoring and reporting is an important component of this framework wherein Shari'ah boards regularly supervise the risk strategy, ensuring transparency to comply with risk appetite and regulatory standards (Ahmed and Khan, 2002).

Challenges to the effective risk management implementation framework in Islamic banking include a lack of uniformity in practices due to the regulatory divergence between jurisdictions and the advancement in the complex risk assessment models dictated by Islamic financial products' hybrid nature. Some instruments have little in terms of historical data, thus leading to a modelling risk with great variance. To deal with such challenges, a sound internal structure has to be developed, investments made in technological aspects, and compliances with international standards of regulations. Global Islamic finance body cooperation can help in the area of harmonization and risk management within the sector (Fadia Fitriyani and Mustafad Ghiffara Ghiffara, 2024).

This entire risk management mechanism assumes importance for the fine developmental avenue and ruggedness of the Islamic banking sector so that they stay safe, compliant, and manoeuvrable in an ever-dynamic financial plane (Van Greuning and Iqbal, 2008).

3. Methodology

3.1 Research Methodology

The research design is predominantly based on secondary research and looks into the implications of cybersecurity risks in the context of digital Islamic banking. The purpose of applying descriptive exploratory research was to assess current literature, regulations, and case studies focusing on vulnerability and risk management practices concerning regulatory considerations of the cyber threats that Islamic financial institutions face.

Secondary data, therefore, widened the research scope and maintained a data-fed phenomenology without the bias or limitations of intermittent primary data collection.

The SLR process was applied to peer-reviewed journal articles and relevant literature, as well as industry reports, policy documents, and publications from the mentioned international financial institutions. High-credibility sources are drawn from the Islamic Financial Services Board (IFSB), International Monetary Fund (IMF), World Bank, Bank for International Settlements (BIS), and Bangladesh Bank, which shed understanding on emerging cyber-risk exposures, regulatory gaps, technological vulnerabilities, and risk mitigation strategies in Islamic banking.

The research organizes the data thematically using content analysis, categorizing them into cyber threats, regulatory frameworks, cybersecurity resilience measures, and Shariah-compliant risk management strategies. Along with content analysis, this study also employs a comparative study of the security of data policies in different jurisdictions to identify best practices that can be transposed to Islamic financial institutions.

This research also followed Takona (2023) thus ensuring a structured secondary research process as regards the data selection methods. Besides, the study relied on alternative credible sources based on academic research, including the Scopus index for journals, Web of Science, Financial Regulatory Reports, and Policy Guidelines.

By collecting only secondary data from existing literature and expert opinions, the research avoids most disadvantages of primary data methods, including the inconvenience in access and biased or unreliable responses. It thus presents a much broader, more objective view of the issues of cyber risk facing Islamic banking and is therefore informative as to the principles underlying risk management itself.

3.2 Data Collecting Method

This study applies a broad-based secondary data evaluation to measure the effect of technology on Islamic financial institutions. The research intends to go into detail with evidence documenting the incorporation of technology into Islamic finance from formal and authenticated sources.

3.2.1 Secondary Data Sources

3.2.1.1 Academic Literature:

- **Peer-Revied Journals and Conference Proceedings:** Digital education, AI governance, Islamic FinTech, blockchain technologies, and computer science are fields under study by peer-reviewed articles and conference proceedings.
- **Research into Shari'ah Compliant Innovations in Technology:** A study is being carried out on innovation in technology with Shari'ah guidelines to get an insight into its impact on Islamic financing practices.

3.2.1.2 Policy Papers and Organizational Reports:

- **Reports from Islamic Financial Institutions:** Reports from Islamic financial institutions, in this case, are primarily from those Islamic banks, which include

Islami Bank Bangladesh Limited (IBBL), Al-Arafah Islami Bank, and Bangladesh Bank for the purposes of analysing their technology-related strategies and implementations.

- **Publications from Governmental Bodies:** The reports to be analysed are those published by the Islamic Development Bank (IDB), the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI), and the Islamic Financial Services Board (IFSB) so that the regulatory structures within which technology conforms to Islamic finance can be understood.

3.2.1.3 Case Studies on Islamic Economies:

- **Comparative Analysis:** Thus, this case study compared the issuance of blockchain Sukuk in Malaysia, Saudi Arabia, and the UAE while also contrasting the AI fatwa system and mobile banking technologies.
- **Research on AI Governance:** Studies analysing the governance of artificial intelligence in some of the key Islamic states as their regulatory mechanisms for Islamic FinTech are explored to bring out the best practices and challenges. Documents from Governments and Industries:

3.2.1.4 Governmental and Industry Reports:

- **The Policy Documents:** This sector reviews the policy instruments on financial inclusion in Bangladesh, digital transformation, and Shari'ah-compliant financial inclusion to understand the government's perspective toward the technological integration of Islamic finance.
- **Technical Procedures:** Documentations of various ministries of Finance, Religious Affairs, and the Central Bank of Bangladesh with respect to Islamic financing, including policy formulations at the national level, have been studied to identify technical regulations.

Thus, this study will aim to analyse all these credibly different sources so that changes and technologies in Islamic finance and governance, thereby opening up endless opportunities and challenges to the industry, may be obtained.

3.3 Sampling Strategy

In qualitative research, especially when using secondary data, 'sampling' refers to the fine selection of specific source data that would commonly apprehend the pervasive criterion of a research query. This is to ensure that the data analysed are information-rich and pertinent to the aims of the inquiry.

Thus, in this type of research, referred to as the secondary data analysis, the sampling strategy is concerned with having data sources readily available to broadly examine digital transformation as it pertains to Islamic banking institutions. Therefore, sources were selected following the criteria below:

3.3.1 Research-Objective Relevance

Only sources that clearly deal with both digital transformation as well as Islamic banking were included as candidates. Examples are studies, reports, and more case analyses that looked at technology within an Islamic financial institution's context.

3.3.2 Credibility and Authority

Sources must be data presented from credible and authoritative bodies like IFSB, IDB or AAOIFI at the maximum adding weight of authority to the evidence being learned. Such repositories stand as credible sources in the documentation and standardization of primary information relevant to this area.

3.3.3 Relevance and Up Datedness

The analysis would focus on the latest update; sources published over the last five years were therefore considered. This age confines even the recent technological advances and regulatory changes touching on Islamic banking.

3.3.4 Scope of Geography

This assembled locations-the studies of such nations, besides Bangladesh in focus, were included because they contain banking frameworks similar to those in Malaysia, Saudi Arabia, and UAE in order to gain a cosmopolitan perspective in trend and practice.

Methodological Rigor: Sources involving strong research designs like empirical studies, systematic reviews, and exhaustive case studies have been prioritized because they assure the reliability and validity of the analysed data.

In so doing, the entire study intends to provide an all-encompassing, multi-faceted reconstruction intending to show how digital transformation affects Islamic banking under a specially designed spotlight on cybersecurity challenges and risk management frameworks.

The data sources play a vital role throughout in analysing and proving the depth and relevance. Contemporaneously, purposive sampling is the widely accepted means of qualitative inquiry for identifying and selecting information-rich cases associated with the phenomenon of interest (Palinkas *et al.*, 2015).

This means that it entails the intentional choice of those sources anticipated to yield maximal insight concerning the research question. Hence, sufficient information-rich cases are concentrated.

Thus, this idea applies particularly to one of the most important issues that develop with qualitative data: the onset of data saturation. Data saturation occurs when, after some point, the gathering of data yields no new term or information concerning the topic, meaning that the topic is sufficiently addressed. Data generated from the analysis using secondary sources can also be said to have reached the saturation point when further investigations of additional sources cease to yield new insights. By this reading, the existing data set indicates that it has reached its limit concerning the research objectives (Wikipedia Contributors, 2025).

So, again, purposive sampling forms part of this study, taking into account the concept of data saturation in that the relevant and comprehensive data sources were selected to keep analysing how digital transformation influences Islamic banking institutions.

3.4 Data Analysis Technique

The research work that is documented in this thesis is primarily directed at the effect of technology on Islamic financial institutions through qualitative data by a variety of methods of analysis. The performance of the analysis is discussed in five sections as shown below:

3.4.1 Thematic Analysis

Thematic analysis sets out to find and interpret patterns in qualitative data. The systematization of textual data to identify reoccurring themes is to make use of this technique for coding and analysis. In this case, thematic analysis helps to explain how the radical changes that occurred with this research affect the different aspects of Islamic finance in terms of Syar'i compliance and operational efficiency.

3.4.2 Content Analysis

Content analysis counts and penetrates the actual content of some specified words, themes, or notions in the data that have been collected. It enables the researcher to determine how often and in what context the term advancement is used in Islamic finance and thus brings a quantitative dimension to qualitative data.

3.4.3 Comparative Analysis

Comparative Analysis is for comparing the technological applications in different Islamic financial institutions. This situational study surveys technologies in banks and financial institutions around Malaysia, Saudi Arabia, and UAE in a bid to rapidly put together points for best practices and challenges met in the implementation of technologies such as Blockchain and artificial intelligence.

3.4.4 NVivo Software Application

For such analyses of complicated qualitative data, the NVivo software is utilized. This data organizes and codes the data such that information is easily retrievable and related across phenomena. The software is, therefore helpful for the researcher to analyse huge amounts of data under a well-structured framework for analysis.

3.4.5 Secondary Data Analysis

There is secondary data analysis where the researcher uses data that are collected by other people or institutions. This is the most cost- and time-effective way for the researcher to answer a new angle or research question by using an existing dataset. The

sources of secondary data are academic literature, policy papers, organization reports, and case studies related to Islamic finance and technology (Wickham, 2019).

3.4.6 Ethical Consideration

Considering the ethics in research carries all through the data analysis process. The researcher ensures that all data remain confidential and, as always, cites the actual source. Besides, the findings are analysed without compromising the integrity of data; there shall be no misrepresentation or selective reporting of findings.

The study, through such methods of analysis, will be able to offer a more specific view of the ways in which technological advancement has been changing Islamic financial institutions and, as such, create a theoretical and practical platform.

4 Findings and Analysis

4.1 Cybersecurity Challenges Identified

Islamic banking in Bangladesh has been facing an overwhelming avalanche of growing challenges in cybersecurity, affecting the operational integrity and security of sensitive customer information stored in such banks. These challenges include the following:

- **High Frequency of Cyberattacks:** In Bangladesh, it is reported that there are, on average, 630 cyberattacks on the banking industry daily, out of which, without hesitation, 52% were termed "high risk" (Afrin, S., 2023).
- **Outdated Banking System:** The bulk of Islamic banks run on the erstwhile banking systems which actually cannot protect against the threats faced on transaction processes since they are much more visible in the light of present or advanced attacks (Temenos, 2023).
- **Increased Digital Banking Vulnerabilities:** The increase in digital banking creates an enhancement of opportunities, therefore raising the call for fool-proof security (Temenos, 2023).
- **Human Error and Manual Process:** Working just on manual processes would often set up room for human error, which can later be exploited by cyber-crooks (Temenos, 2023).
- **Regularity Challenges**: Islamic banks rely on regulators to enlighten them on the issue of measures, but it is said that, in this fast-evolving technological tongue, regulators are almost always lagging behind (Temenos, 2023).
- **Insider Threats:** Research indicates that 58% of all insider-related occurrences in organizations occur as a consequence of inadvertent actions like system misconfigurations and excessive insider sharing (Temenos, 2023).
- **Underinvestment in Cybersecurity**: It is common knowledge that hefty amounts were spent on IT infrastructure, some even to the degree of saying that not much was allocated to security. From a different point of view, only 5% of Tk1,666 crore spent on IT in the banking sector went to security measures in 2020 (Afrin, S., 2023).

- **Data Exposure:** An alarming number of issued bank cards are being sold on the dark web from Bangladesh; this exposes financial institutions and account holders to possible financial losses (Afrin, S., 2023).

These varieties of challenges provide an opportunity for Islamic banks in Bangladesh to upgrade and modernize their IT infrastructure, implement advanced cybersecurity, and install security awareness in their employees, etc.

4.2 Risk Management Practice

It is actually a real challenge for the Islamic banks in Bangladesh. The banks have such extreme strictness and apply everything which is these over-the-top risk management techniques. Here are some of the major standards that they have been applying:

- **Framework for Consistent Risk Management:** The risk management framework by banks covers a strategic policy framework plus procedures and governance structures for the identification, assessment, and management of risk. For instance, investment exposure and operational vulnerabilities were framed into risk management-based modelling by Islami Bank Bangladesh Limited (IBBL) (Uddin and Akther, 2015).
- **Zero Trust Security Model for Access Control:** With this model of zero trust, access is always granted through creating evidence of identity verification reducing the risk of unauthorized access where a zero-trust model is installed. This concept revolves around active preventive means of cybersecurity rather than passive defence against it (Temenos, 2023).
- **Adoption of AI:** AI systems are beginning to analyse network activities and create gain signatures that will create an understanding of an anomalous stat that an anomaly might represent a threat to cyberspace. Once the threat is caught, early spotting and remedy give cushion time to act (Temenos, 2023).
- **Adoption of FinTech:** Fintech is efficient in having the best customer engagement through machine analysis of data and automating processes. It hence advances risk profiling with greater operational efficiency and better compliance, among others, for managing risks (Al Hammadi *et al.*, 2024)
- **Collaboration with Regulatory Authority:** It's all about the banks coordinating with the respective regulatory authorities that could buffer banks while most of the changes in mandatory compliance have been assimilated in today's reality, including changing threats emerging. Meanwhile, putting meaningful collaborations that would not be trivial at all in work were also their universities (Rahman, Rahman and Azad, 2015).
- **Employee Education and Awareness Training:** Humans are by far the biggest focus in any cybersecurity operation, and this is precisely the reason that has made banks invest heavily in various kinds of training programs regarding security protocols, phishing attacks, and safe online practices to minimize human error leading to breaches.

- **Periodic Security Audit and Assessment**: They are auditing and assessing continuously every pitcher and identifying weak zones for remediation as soon as possible. Thus, this Appraisal will be continuous over time; it will be effective against a brigade of attacks that can change every moment.
- **Incident Response Planning**: They are detailed action plans based on numerous scenarios that go beyond the mere cyberattack incident response. These plans will allow an immediate reaction to halt breaches and damage before recovery begins.

Such risk management practices shall be instrumental in ensuring that Islamic banks in Bangladesh will continue to strengthen themselves in terms of cybersecurity and insulation from potentially emergent cyber threats all in the greater interest of safeguarding stakeholders and with the resilience of financial systems.

4.3 Comparison with Global Standards

This section provides a critical analysis of Islamic bank practices in Bangladesh in relation to international standards, focusing on converging zones and, thus, future improvement prospects.

4.3.1 National Directives

The Bangladesh Bank, being the apex regulatory authority, has laid down exhaustive measures through detailed guidelines to all financial institutions to beef up their cybersecurity posture. The "Guideline on ICT Security" provides specific information and communications technology (ICT) risk management requirements with strong security controls, monitoring, and incident response requirements. The direction outlined was intended to fortify the financial institutions against cyberattack threats.

4.3.2 Alignment with International Standards

The wide range of cybersecurity standards recognized internationally in the financial institutions sector is designed to protect sensitive information while maintaining systemic stability. Just a few of the foremost among them are:

- **ISO/IEC 27001:** International standard requiring the establishment, implementation, maintenance and continuous improvement of an information security management system, including risk assessment and treatment processes and periodic auditing for compliance.
- **NIST Cybersecurity Framework:** This part provides guidance in policies' framework computer security assessing and improving their capability to prevent, detect, and respond to attacks in their systems.
- **Basel Committee on Banking Supervision (BCBS) Directives**: Principles of resilience, operational and management standards sound a well-defined operational risk cover all specific directives as far as cyber risk banking is concerned.

All these standards are used to develop cybersecurity practices for Islamic banking in Bangladesh.

4.3.3 Risk Management Frameworks: As ISO/IEC27001, banks have a complete risk management framework established to conduct periodic assessments where security controls are instituted and constantly monitor vulnerability.

4.3.4 Zero Trust Security Model

A "Zero Trust" model always requires more and stricter access verification of individual identities in the banks adopting an advanced posture.

4.3.5 Artificial Intelligence for Threat Detection and Response

In addition to monitoring network activities analysing data patterns, and perceiving anomalies, AI systems will generate threats for identifying and responding to them.

4.3.6 Opportunity for Enhancement

As much as the globe has quite a myriad of internationally astute perspectives, such could be:

- **Strengthening Regulatory Frameworks:** These regulations, being more and more specific, thus should now be continuously updated because there are always new risks coming up on the online front, and also, improvements in the best practices and their standards should find their way into the national directives (Almansi, Aquiles A., 2025).
- **Capacity Building and Training**: Investments in customized training will ensure that current personnel in the field of cybersecurity are outfitted with the contemporary tools and techniques, including global standards, that will significantly reduce the chances of a security breach across the institution.
- **Advanced Threat Intelligence Sharing**: There would be far more chances of anticipating and controlling cyber threats if sharing regarding threats is enhanced among nations and internationally.

4.4 Gaps and Area Improvement

This marks a significant change in the cyber defence architecture of banking in Bangladesh, but there are a lot more things that need to be done before the country can stand side by side with its international counterparts to face new threats.

4.4.1 Weak Regulatory and Legal Infrastructure

The regulatory and legal set-up of Bangladesh has proven to be very weak in addressing the complex nature of the cybersecurity threats, which have made them insurmountable for most financial institutions. The systems in place make themselves indifferent to the unique differences of a system and endanger the entire sector with very sophisticated cyber-attacks. According to the study, there must be flexible and sufficient regulatory environments from which protective mechanisms against such threats can be developed (Hossain and Hasan, 2023).

4.4.2 Lack of Cybersecurity Awareness and Training

Ignorance and lack of training are two major human factors responsible for almost all cyber vulnerabilities concerning banks. There is a serious need to erect an integrated education and training initiative for the bank personnel to combat threats. Continuous training and awareness programs would minimize human error-initiated breaches (Mamun, Bin and Sk Mamun Mostofa, 2022).

4.4.3 Lack of Incident Response and Recovery Mechanisms

The lack of measurable and scientifically definable incident handling and recovery is the main cause of aggravating other incidents against financial institutions. The $81 million that hackers made in stealing from Bangladesh Bank in 2016 is evidence enough to bear testimony on the incident response need. It is very important to develop and keep updating these strategies in time for when the occasion demands it so there would be an implementation at any time it would be necessary in case of a security breach (Balu, 2023).

4.4.4 Limited Investment in Advanced Cybersecurity Technologies

The major hindrance that blocks Islamic banks in Bangladesh from investing in the latest cybersecurity technology is primarily limited to issues of budgetary constraints. Therefore, it has made access to the latest solutions, such as AI-enabled threat detection systems, current encryption protocols, and models of multifactor authentication. Hence these banks should take the investment in the advancement of such technologies as one of their organizational first priorities to mount effective resistance against emerging cyber threats.

4.4.5 Lack of Cooperation and Information Sharing

There is a focus on cooperation and information sharing among financial institutions when it comes to cybersecurity threats and best practices. This poses an alarming concern, considering the need to establish a forum for constant dialogue and cooperation regarding the sharing of threat intelligence and addressing any definable areas of vulnerability on the part of banks. Such collaboration would also provide immense help in fighting against common adversaries in the cyberspace sector.

4.5 Suggestions for Betterment

For anything meant to fill the suggested gap, the next few steps become recommendations:

- **Strengthening of Regulatory Frameworks:** Governments and regulators within the public sector should work toward more comprehensive cybersecurity policies concerning prevention from threats when they evolve. The latter should also allow for any of those regulations that might require security practices in dossiers with respect to regular compliance audits.
- **Enhancing the Training Programs:** In terms of an awareness campaign raising mobility and skill-building in issues related to cybersecurity, financial institutions

should continually invest in training and specialized training for employees. An internal training initiative such as this will foster a culture of security among all staff members and hence reduce opportunities for exploitation of human vulnerabilities.

- **Development of Good Incident Response Strategies:** Banks need to develop their Incident Response Plans and Disaster Recovery Plans and regularly test them through simulations to demonstrate preparedness and minimize the impact of any eventual incident.
- **Investing in Advanced Technologies:** Advanced cybersecurity solutions: AI-based analytics, real-time threat-monitoring systems, and strong encryption require funding that needs to be mobilized in the Islamic banks to strengthen their security.
- **Promoting Inter-Woven Institutional Collaboration:** Setting up forums and networks for information sharing among banks will return a resilient financial sector. This represents cooperation in intelligence sharing, and coordinated responses would strengthen the overall cybersecurity framework.

If these areas are addressed effectively, they will prove effective in safeguarding assets and the savings of the fast-changing digital financial ecosystem before Islamic banks' high and low presence in Bangladesh even recognizes themselves.

5. Discussion

5.1 Impact on Customer Security Trust

The essence of a satisfactory cyber environment rests with the Islamic banking institutions gaining and sustaining customer trust, which puts the utmost importance on cybersecurity. Security is the crux that fosters customer trust: safeguarding the sanctity of personal sensitive data and financial transactions.

5.1.1 Cybersecurity as a Building Block of Trust

Research has established that trust/insecurity from the consumer perspective in the domain of banking services is built on the foundation of cybersecurity. For example, it was found that customers' awareness concerning cyber disturbances may greatly impact their trust and commitment toward their banks. Conversely, good market performance and trustworthiness among customers characterize those banking institutions which are known to communicate such measures and incidents proactively (Ishtiaq Ahmad Bajwa *et al.*, 2023).

5.1.2 Consequences for Islamic Banks

With Shariah guidelines at the heart of its functioning, Islamic banking is threatened whenever there is a cyber incident. It’s very increased computerization of Islamic banking services presents a relatively wider attack surface, thus rendering the aspects of cyber security even more pertinent. An example worth citing is the Bangladesh Bank cyber-

heist case, which has been destructive in triggering the erosion of public confidence in the banking industry - a serious financial loss. Therefore, shortly disclosed high-level cyber-risk disclosures by the banks became essential for the restoration of the legitimacy of trust.

5.1.3 Strategies to Enhance Customer Trust Through Cybersecurity

- **Advanced Security Technology Deployment:** The security framework can be hardened with real-time detection and response to threats using AI and ML tools (Temenos, 2023).
- **Regular Security Audits and Transparency:** Periodic assessments of security posture resulting in the clear communication of findings to clients could build trust - an open book in documenting methods of cybersecurity will speak to the institution's commitment toward consumer interests.
- **Education and Awareness:** An introduction to knowledge of possible cyber threats and safe banking practices will empower the customers, thereby increasing their confidence in protecting their information and trust in the institution.

5.2 Regularity Implications

Envisioning the comprehension of embedding Islamic cyber security has a much broader regulatory impact regarding the Bangladesh central banks. As such, bringing into place rules, regulations, and guidelines in Bangladesh Bank enables for increased strengthening of the cyber-security architecture of financial institutions.

5.2.1 Key Regulatory Initiatives:

- **Creation of Cyber Security Unit (CSU):** Bangladesh Bank incorporated the CSU in May 2020 with mandates to monitor and strengthen the cybersecurity profile of banks and financial institutions starting July 2019 (Bank, 2019).
- **Issue of the Guideline on ICT Security:** The core or sole mandate of this unit is to issue the “Guideline on ICT Security”. These include assignments for the management of banks, permanent monitoring of the strategic objectives of banks supported by IT, awareness of ICT risks, and compliance with the various regulatory requirements as imposed by Bangladesh Bank in its localized issues in the title "Guideline on ICT Security for Banks and Financial Institutions” (Bank, 2023).

5.2.2 Identified Challenges:

- **Inadequate Regulatory Frameworks:** The current regulatory and legal frameworks of Bangladesh have been proven by studies to be gravely insufficient to address most of the matters that are linked to cybersecurity within financial institutions. Existing frameworks would thus seem significance-hollow enough not to reasonably counteract the advanced cyber threats.

5.2.3 Comparative Insights:

- **Global Standards:** Strict cyber security laws have been adopted in different jurisdictions. For example, the Central Bank in Bahrain requires Islamic banks to conduct periodic audits and to have independent Cybersecurity Risk Function reporting to executive-level management, among other initiatives with regard to advanced threat detection systems.

5.2.4 Recommendations:

- **Strengthening Regulatory Measures:** An urgent need exists for Bangladesh to come out with an elaborate and strong regulatory framework. This framework should not only build a secure environment for cyber threats facing financial institutions but also encourage consumer confidence in such banking services.

5.3 Comparative Insight

A comparative analysis in cyber security enumerated the degrees of regulatory maturity and implementation of jurisdictions across the Islamic banking system. Bangladesh has made timid strides towards bolstering cybersecurity in its financial sector, while other jurisdictions have harmonized opposition in increasingly comprehensive and stringent terms.

5.3.1 Bangladesh: Emerging Frameworks:

- **Cyber Security Unit:** CSU: The Bangladeshi Bank started its Cyber Security Unit in July 2019 and became operational in May 2020, governing and improving the cybersecurity posture of the banks and financial institutions (Bank, 2019).
- **Guidelines on ICT Security:** The purpose of this guideline issued by the Bangladesh Bank is to designate the responsibilities of management in banks in continuously monitoring IT-related strategic goals, knowing ICT risks and complying with regulatory requirements (Bank, 2023).

5.3.2 Global Practices: Extreme Measures:

- **Bahrain**: According to the Central Bank of Bahrain, Islamic bank licensees should maintain an independent cybersecurity risk function distinct from the IT department, which should report to senior management on the status and maturity of its cybersecurity controls (Central Bank of Bahrain, 2022).
- **Pakistan**: In terms of cybersecurity, cloud storage, or advanced data analytics, the regulation requires at least one member of the Board to have such knowledge. They will then require the Islamic banks to observe current technology and cloud storage and cybersecurity-related standards (Islamic Financial Services Board, 2023).
- **Mauritius**: Islamic banks should comply with data protection laws and establish appropriate cyber and technology risk management frameworks to safeguard their business (Islamic Financial Services Board, 2023).

5.3.4 Key Observations:

- **Regulatory Maturity:** Countries such as Bahrain and Pakistan have moved up the ladder to enact highly advanced cybersecurity legislation in the domain of Islamic banking as an early response to the threats perceived in the digital realm.
- **Board-Level Expertise:** Cyber-security Board-level expertise becomes a prerequisite in Pakistan, so that the institution can take into consideration cyber risks in its broader strategic decision-making. It would also enhance the security posture of the institution.
- **Comprehensive Risk Management:** The accent on having independent cybersecurity functions and risk management frameworks stands out in the case of Bahrain and Mauritius, where dedicated resources and structured approaches to cybersecurity are necessitated.

5.3.5 The Implications for Bangladesh

Bangladesh has shown considerable progress in terms of establishing the fundamental requirements for cybersecurity. In addition, improvements to and extensions of these would take the country into a significantly broader realm of frameworks. Independent cybersecurity capabilities and activities, board-level interest in cybersecurity, and additional risk management measures following global best practices would greatly strengthen Bangladesh's Islamic banks against cyber threats.

It says that Bangladesh ought to become proactive and regimented in established approaches, owing to the global standing on the situation in cybersecurity vis-à-vis Islamic banking against dangerous, tedious threats.

6. Conclusion

6.1 Summary of Key Findings

The research works toward accomplishing a holistic and detailed review of the cyber security practice in Bangladesh Islamic banks against global standards to explore the challenges and improvement avenues. The key findings are:

- **Cyber Security Challenges Identified:** The Islamic banks are not free from the ill effects of their own. The effects were glaringly evident in the incident when $81 million was illegally transferred in the name of compromised SWIFT network credentials in 2016 by Heist Bangladesh Bank. This incident reflects the gaps in the cyber-defined system of the banking sector (Balu, 2023).
- **Risk Management Practices:** Bangladesh Bank's measures include setting up a Cyber Security Unit (CSU) in 2019 and issuing the "Guideline on ICT Security for Banks and Financial Institutions." Broadly, this is to counteract state cyber threats and further outline management responsibilities for banks with respect to regulatory compliance and monitoring of IT strategic goals.

- **Comparison with Global Standards:** Bangladesh lays a foundation level on which all the other jurisdictions have started, considering the fact that other countries now have even heavier hands in implementation and the framework. The edict from the Central Bank of Bahrain, for instance, instructs that independent cybersecurity risk functions set up for Islamic banks should report directly to top management.
- **Gaps and Areas for Improvement**: The future is said to be rosy, too, with its challenges, and there exist gaps, as present regulations and the legal framework of Bangladesh do not provide a very strong demand against the diversity of needs that a financial institution faces in the cyber world by virtue of being an institution. Well-in-time policies defining effective measures are needed to counter the diversity of advanced classes of cyber threats.

6.2 Contribution to Theory and Practice

This is a significant article with respect to theory and practice in cybersecurity in the context of Islamic banking in the banking industry in Bangladesh.

6.2.1 Theoretical Contributions:

- **Integration of Cybersecurity and Islamic Banking Literature**: The research serves to understand the implications of cyber threats on Sharia-compliant financial institutions with respect to examining the cybersecurity challenges facing the Islamic banks of Bangladesh. Thus, it fills an important gap in the discussions on cybersecurity and Islamic finance literature.
- **Insights into Cybersecurity Disclosure Practices:** The relevance of voluntary disclosures on cybersecurity to the banking sector is discussed in this research as how meaningful and transparent communication of cyber risks can help in building trust among stakeholders and brightening better regulatory policy (Mazumder and Hossain, 2022).
- **Impact of Cybercrime Sentiments on Technology Adoption**: The study on how sentiments of cybercrimes impact the adoption behaviour of customers with respect to mobile banking services at Islamic banks adds to the larger debate on technology acceptance models, especially with respect to Islamic financial institutions (Kornitasari, Sura and Dewi, 2024).

6.2.2 Practical Contributions:

- **Framework for Strengthening Cybersecurity Measures:** On practical grounds, these are findings that give a framework for Islamic banks in Bangladesh directed towards the assessment and strengthening of their cybersecurity infrastructures, emphasizing the need for extensive risk management practice and strategy for active threat hunting.
- **Policy Advice to Regulatory Bodies:** The research gives directives to policymakers and regulatory bodies, including Bangladesh Bank, to develop the

guidelines on cybersecurity in line with the modus operandi of these Islamic banking institutions.

- **Advice on Cybersecurity Disclosure:** It describes how cybersecurity disclosures may indeed augment customers' trust with recommendations for banks on how to inform their key stakeholders regarding cybersecurity matters.

6.3 Recommendations for Future Research

The study results will leave future research areas open, which can, in turn, contribute to enriching the understanding of cybersecurity in Islamic banking in Bangladesh:

- **Examining Future Technological Solutions:** An investigation on how machine learning and deep learning can be integrated to improve the defences of cybersecurity. This may also consider the contribution of these technologies to fraud detection, malware detection, and intrusion prevention, specifically for Islamic banks (Md. Badiuzzaman Biplob, Bhuiyan and Farabi, 2024).
- **Effects of Cybersecurity Disclosures**: This can be one area of future research on how the level of disclosure of cybersecurity information affects bank performance. Others may investigate how voluntary disclosures of cybersecurity practices may affect customer trust, financial soundness, and adherence of Islamic banking institutions to their requirements (Elsayed, Ismail and Ahmed, 2024).
- **Comparative Study of Regulatory Frameworks:** This would ideally involve a comparative analytical approach to the regulatory regimes of digital banks and Islamic digital banks in Bangladesh as well as in other countries. This will help in setting best practices and emphasize regulatory gaps to draw useful conclusions on the best policy frameworks to support cybersecurity resilience (Salim, Masukujjaman and Nor, 2024).
- **Fintech and Its Role in Risk Management:** The effect brought in by fintech in risk management on Islamic banks. The study will investigate how the innovation in fintech has impacted the risk measure, risk mitigation, and operational efficiency of Sharia-compliant financial institutions (Ishtiaq Ahmad Bajwa *et al.*, 2023).
- **Cybersecurity Risk Analysis**: A sound risk assessment has to be set regarding Islamic banking that defines general threat sources, evaluates the efficiency of risk measures and proposes addressing possible artificial threats to Islamic financial institutes.

Not only would this justification of the proposed research paths add to the quiet academic debates among Islamic banking pertinent to cyber insecurity, but it would convert into well-informed applications for action by practitioners and policymakers as to what actions should be taken toward resilience in financial institutions.

Conflict of Interest Statement
The authors declare that there is no conflict of interest regarding the publication of this article. The research was conducted independently, without any financial, personal, or professional affiliations that could influence the findings or interpretations. No external funding was received for this study.

About the Author(s)

Ebrahim Mollik is a master's student in International Business with Data Analytics at Ulster University, UK. His research interests include the intersection of technology and Islamic finance, particularly in the context of Bangladesh. Ebrahim's work focuses on exploring the role of technological innovation in enhancing financial governance, financial inclusion, and education in Islamic finance. His research aims to provide insights into how digital transformation can shape the future of Islamic finance, fostering greater financial inclusion in emerging markets.
Dr. Faisal Majeed is an experienced Business Management Lecturer and Dissertation Supervisor with over 10 years of expertise in teaching, research, and management, both locally and internationally. He holds a Ph.D. in Business Management from the University of Bolton and an M.Sc. in International Business and Management from the University of Bedfordshire. With a background in Marketing (MBA) and proficiency in English, Dr. Majeed possesses excellent communication, leadership, and organizational skills. He is dedicated to fostering academic excellence and supporting students in their careers, combining innovative teaching methods with practical industry insights.

References

31st anniversary issue-I (2025). *The Financial Express*. [online] The Financial Express. Available at: https://thefinancialexpress.com.bd/editorial/ensuring-cyber-security-of-banks [Accessed 20 Feb. 2025].

Afrin, S. (2023). *Cybersecurity Challenges in Bangladesh's Financial Sector*. [online] The Daily Star. Available at: https://www.thedailystar.net/supplements/digital-transformation-bangladeshs-financial-industry-2023/news/cybersecurity-challenges-bangladeshs-financial-sector-3475851.

Afrin, S. (2023). *The Daily Star*. [online] The Daily Star. Available at: https://www.thedailystar.net/supplements/digital-transformation-bangladeshs-financial-industry-2023/news/cybersecurity-challenges-bangladeshs-financial-sector-3475851 [Accessed 19 Feb. 2025].

Ahmed, H. and Khan, T. (2007). *0 Risk management in Islamic banking*. [online] Available at: https://www.isfin.net/sites/isfin.com/files/risk_management_in_islamic_banking.pdf

Al Hammadi, M., Jimber-Del Río, J.A., Ochoa-Rico, M.S., Montero, O.A. and Vergara-Romero, A. (2024). Risk Management in Islamic Banking: The Impact of Financial Technologies through Empirical Insights from the UAE. *Risks*, [online] 12(2), p.17. doi: https://doi.org/10.3390/risks12020017.

Asian Banking & Finance (2023). *The resilience and growth of Islamic Banking in Bangladesh*. [online] Available at: https://asianbankingandfinance.net/islamic-banking/commentary/resilience-and-growth-islamic-banking-in-bangladesh

Balu, R. (2023). *Bangladesh Bank Cyber Heist*. [online] Georgia Tech Repository. Available at: https://repository.gatech.edu/server/api/core/bitstreams/df3d1c19-47be-4738-a855-9c049b709d52/content

Bank, B. (2019). *Bangladesh Bank*. [online] Bb.org.bd. Available at: https://www.bb.org.bd/en/index.php/about/deptdtl/7 [Accessed 22 Feb. 2025].

Bank, B. (2023). *Guideline on ICT Security Bangladesh Bank*. [online] Available at: https://www.bb.org.bd/aboutus/draftguinotification/guideline/draft_ictpolicy.pdf [Accessed 22 Feb. 2025].

Bank, B. (2023). *Guidelines For Conducting Islamic Banking. Section I Introduction to Islamic Banking*. [online] Available at: https://www.bb.org.bd/aboutus/regulationguideline/islamicbanking/guideislamicbnk.pdf [Accessed 19 Feb. 2025].

BIBM (2021). *Academic Calendar 2021 Bangladesh Institute of Bank Management*. [online] Available at: https://www.bibm.org.bd/upload/academic_calendar/AC-2021.pdf [Accessed 20 Feb. 2025].

Central Bank of Bahrain (2022). *Entire Section | Rulebook*. [online] Thomsonreuters.com. Available at: https://cbben.thomsonreuters.com/entiresection/211765 [Accessed 22 Feb. 2025].

CIBAFI (2021). *CIBAFI Briefing*. [online] Available at: https://www.cibafi.org/Files/L1/Content/CI2146-CIBAFI%20BRIEFING%2015%20%283%29.pdf [Accessed 20 Feb. 2025].

CSIB (2020). *CSBIB – Central Shariah Board for Islamic Banks of Bangladesh*. [online] CSBIB. Available at: https://csbib.org/new [Accessed 19 Feb. 2025].

CYBLE (2024). *Securing Data in Islamic Banking: Case Study on Compliance*. [online] Cyble. Available at: https://cyble.com/threat-intelligence-for-bfsi/securing-data-islamic-banking [Accessed 20 Feb. 2025].

Elsayed, D.H., Ismail, T.H. and Ahmed, E.A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, 10(1). doi: https://doi.org/10.1186/s43093-024-00402-9.

Fadia Fitriyani and Mustafad Ghiffara Ghiffara (2024). *Risk Management in Islamic Banking: Challenges and Management Strategies*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/377113118_Risk_Management_in_Islamic_Banking_Challenges_and_Management_Strategies#fullTextFileContent [Accessed 20 Feb. 2025].

Habiba Nowrose (2024). *The Daily Star*. [online] The Daily Star. Available at: https://www.thedailystar.net/supplements/islamic-banking-bangladesh/news/the-future-islamic-banking-bangladesh-3741086

Hossain, M. (2022). *Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh*. [online] Available at: https://dspace.bracu.ac.bd/xmlui/bitstream/handle/10361/21785/22141066%2C%2018301283%2C%2018301258%2C%2018301101_CSE.pdf [Accessed 19 Feb. 2025].

Hossain, M.A. and Hasan, M.R. (2023). A Simplified Cybersecurity Policy Framework for the Financial Institutions in Bangladesh: A Survey of Literature. [online] XLII(03), pp.41–81. doi: https://doi.org/10.3329/dujbst.v42i3.65120.

Ishtiaq Ahmad Bajwa, Ahmad, S., Mahmud, M. and Farooq Ahmad Bajwa (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Information & computer security*, 31(5). doi: https://doi.org/10.1108/ics-11-2022-0179.

Islamic Financial Services Board (2023). *IFSB Working Paper Series Wp-27/12/2023 Regulatory Practices in Digital Islamic Banking*. [online] Available at: https://www.ifsb.org/wp-content/uploads/2023/12/WP-27-Regulatory-Practices-in-Digital-Islamic-Banking.pd

Kornitasari, Y., Sura, L.J. and Dewi, D.N.A.M. (2024). How cybercrime sentiment shapes mobile banking adoption in Islamic banking. *Jurnal Ekonomi & Keuangan Islam*, pp.217–232. Doi: https://doi.org/10.20885/jeki.vol10.iss2.art6.

Mamun, A.A., Bin, J. and Sk Mamun Mostofa (2022). Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies. [online] 9(1), pp.88–94. Available at: https://www.researchgate.net/publication/362365065_Cyber_Security_Awareness_in_Bangladesh_An_Overview_of_Challenges_and_Strategies#fullTextFileContent.

Mazumder, M.M.M. and Hossain, D.M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? *Journal of Accounting in Emerging Economies*. Doi: https://doi.org/10.1108/jaee-07-2021-0237.

Md. Badiuzzaman Biplob, Bhuiyan, T. and Farabi, A.M. (2024). Using Machine Learning and Deep Learning to Strengthen Bangladesh's Financial Infrastructure for Banking Cybersecurity. [online] doi: https://doi.org/10.20944/preprints202409.0645.v1.

Palinkas, L., Horwitz, S., Green, C., Wisdom, J., Duan, N. and Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, [online] 42(5), pp.533–544. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC4012002/.

Rahman, M.M., Rahman, Md.A. and Azad, Md.A.K. (2015). Risk Management Practices in Islamic and Conventional Banks of Bangladesh: A Comparative Analysis. *Asian Social Science*, 11(18). doi: https://doi.org/10.5539/ass.v11n18p153.

Report, T.T. (2022). *Majority of banks at high cyber risks: BIBM study*. [online] The Business Standard. Available at: https://www.tbsnews.net/economy/banking/majority-banks-high-cyber-risks-bibm-study-438594 [Accessed 19 Feb. 2025].

Salim, A.S., Masukujjaman, M. and Nor (2024). A Comparative Study on the Regulations for Establishing Digital Bank and Islamic Digital Bank: Bangladesh vs Malaysia. *5th UUM International Islamic Business Management Conference*. [online] Available at: https://www.researchgate.net/publication/384087677_A_Comparative_Study_on_the_Regulations_for_Establishing_Digital_Bank_and_Islamic_Digital_Bank_Bangladesh_vs_Malaysia.

Takona, J.P. (2023). Research design: qualitative, quantitative, and Mixed Methods Approaches / Sixth Edition. *Quality & Quantity*, [online] 58(1), pp.1011–1013. doi: https://doi.org/10.1007/s11135-023-01798-2.

Temenos (2023). *Detecting and Preventing Cybercrime in Islamic Banks*. [online] Temenos. Available at: https://www.temenos.com/news/2023/12/13/detecting-and-preventing-cybercrime-in-islamic-banks [Accessed 20 Feb. 2025].

Tim Maurer and Arthur Neloson (2021). *The Global Cyber Threat to Financial Systems – IMF F&D*. [online] Imf.org. Available at: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer

Uddin, M. and Akther (2015). *Munich Personal RePEc Archive Risk Management Practices in Islamic Bank: A Case Study of Islami Bank Bangladesh Limited*. [online] Available at: https://mpra.ub.uni-muenchen.de/68781/1/MPRA_paper_68781.pdf [Accessed 22 Feb. 2025].

V. Sundarajan and Luca Errico (2002). Islamic Institution and Product in the Financial System. Available at: https://www.imf.org/external/pubs/ft/wp/2002/wp02192.pdf

van de Vann, P.-J. (2024). *How Digital Solutions Are Driving the Growth of Islamic Banking*. [online] Hexaware –. Available at: https://hexaware.com/blogs/islamic-banking[Accessed 20 Feb. 2025].

Van Greuning, H. and Iqbal, Z. (2008). *Risk Analysis for Islamic Banks*. [online] Available at: https://documents1.worldbank.org/curated/fr/688471468143973824/pdf/424810PUB00ISB101OFFICIAL0USE0ONLY1.pdf

Wickham, R. (2019). Secondary Analysis Research. *Journal of the Advanced Practitioner in Oncology*, [online] 10(4), pp.395–400. doi: https://doi.org/10.6004/jadpro.2019.10.4.7.

Wikipedia Contributors (2019). *Bangladesh Bank robbery*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery.

Wikipedia Contributors (2025). *Sample size determination*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Sample_size_determination