BIISS JOURNAL, VOL. 46, NO. 2, APRIL 2025: 199-220
DOI: https://www.doi.org/10.56888/BIISSj2025V46n2a3
ISSN: 1010-9536 (Print)

Muhammad Mazedul Haque

AI IN THE CROSSHAIRS: AN ASSESSMENT OF AI-BASED CYBERSECURITY THREATS IN BANGLADESH

Abstract

This paper explores the cybersecurity risks posed by Artificial Intelligence (AI) technologies in Bangladesh, focusing on personal data security, health sector, and human resources sector. Using qualitative methods, including literature reviews, key informant interviews, and case studies, this study examines AI-driven or for the first area and adversarial machine learning attacks for the two sectors, along with factors contributing to vulnerabilities from such threats. Bangladesh does not face significant cybersecurity challenges from AI-based cyber threats due to limited resources of cyber attackers that would utilise AI-based tools, an overall lower cyber literacy, and a shortage of skilled professionals among cyber criminals due to the novel nature of this relatively new technology. This is all despite the rapid pace of AI adoption outstripping the development of robust cybersecurity strategies, leaving organisations and individuals vulnerable to new threats. This research aims to explore any existing AI-related cybersecurity threats in Bangladesh, propose targeted mitigation strategies, and provide recommendations for policymakers, cybersecurity practitioners, and other stakeholders. Despite the currently insignificant threat of AI-based cyber threats, this study highlights the urgent need for comprehensive measures to safeguard digital infrastructure and assets. By enhancing the understanding of AI-related cybersecurity risks and proposing effective preventive measures, this study seeks to strengthen Bangladesh's resilience against emerging AI-driven threats, ensuring the continued security and stability of the nation's digital landscape.

Keywords: AI-based Cyber Threats, Cybersecurity, AI-based Cyber Attacks, AI Adoption, Cyber Literacy.

1. Introduction

With the rapid advancement and integration of Artificial Intelligence (AI) technologies across various sectors, the landscape of cybersecurity[1] is undergoing significant transformations. As AI systems become increasingly prevalent in

Muhammad Mazedul Haque is Research Officer, Bangladesh Institute of International and Strategic Studies (BIISS). His email address is mazedul@biiss.org

[1] I.e., ongoing developments related to cybersecurity.

Bangladesh, they bring unprecedented opportunities and formidable challenges in cybersecurity. This paper aims to investigate the cybersecurity vulnerabilities posed by AI technologies in the context of Bangladesh, along with exploring prospects for enhancing cybersecurity resilience in the country.

Artificial intelligence encompasses a range of technologies that enable machines to perform tasks that traditionally require human intelligence, such as problem-solving, decision-making, and pattern recognition. In recent years, AI has witnessed widespread adoption in diverse domains, including finance, healthcare, transportation, and governance, among others. In Bangladesh, the uptake of AI technologies is evident across various sectors,[2] driven by initiatives to enhance efficiency, productivity, and innovation. However, alongside the proliferation of AI comes the emergence of new cybersecurity threats and vulnerabilities. AI-powered attacks, such as adversarial machine learning, AI-driven phishing[3], and manipulation of AI algorithms[4], pose significant risks to digital infrastructure and sensitive data. These threats are compounded by the evolving cybersecurity landscape in Bangladesh, characterised by a complex interplay of socioeconomic, regulatory, and technological factors.

Despite efforts to bolster cybersecurity measures, Bangladesh faces several challenges in mitigating AI-related cybersecurity risks. Limited resources, inadequate regulatory frameworks, and a shortage of skilled cybersecurity professionals exacerbate the vulnerability of digital systems to malicious activities. Moreover, the

[2] AI is being tested for diagnosing diseases in trial testing at centres such as the Kurmitola General Hospital, Dhaka, Bangladesh. For details see, Badiuzzaman Pranto, Sk Maliha Mehnaz, Esha Bintee Mahid, Imran Mahmud Sadman, Ahsanur Rahman and Sifat Momen, "Evaluating machine learning methods for predicting diabetes among female patients in Bangladesh," Information 11, no. 8 (2020): 374; It is being tested in the pharmaceuticals industry for prescription medicine allocation by companies such as Genofax. For details see, Nurul Islam Hasib, "Genofax aims Bangladesh for big data driven medicine," *Dhaka Tribune*, November 11, 2023, accessed December 20, 2023, https://www.dhakatribune.com/bangladesh/330736/genofax-aims-bangladesh-for-big-data-driven; Companies such as Bkash and Unilever are using AI models in their HRM to enhance the skills of their workers. For details see, Shamim Ahmed, "Bringing AI, analytics in Bangladesh to the fullest," *The Business Post*, May 07, 2023, accessed November 23, 2023, https://businesspostbd.com/business-connect/bringing-ai-analytics-in-bangladesh-to-the-fullest-2023-05-07.

[3] Phishing has been defined as *"a scalable act of deception whereby impersonation is used to obtain information from a target".* For details see, Elmer EH. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Science* 3, no. 1 (2014): 1–10.

[4] An algorithm refers to a set of rules or instructions designed to solve a specific problem or perform a particular task within the context of securing computer systems, networks, and data. These algorithms can range from cryptographic algorithms used to encrypt and decrypt data to detection algorithms used in intrusion detection systems (IDS) or antivirus software. For more see, Srivaths Ravi Anand Raghunathan, Paul Kocher and Sunil Hattangady, "Security in embedded systems: Design challenges," *ACM Transactions on Embedded Computing Systems (TECS)* 3, no. 3 (2004): 461–491; See also, Priyanka Dixit and Sanjay Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Computer Science Review* 39 (2021): 100317.

rapid pace of technological advancement often outpaces the development of robust cybersecurity strategies, leaving organisations and individuals susceptible to emerging threats.

In light of these developments, there is an urgent need to comprehensively examine the intersection of AI and cybersecurity in Bangladesh. By identifying vulnerabilities, understanding underlying factors, and proposing mitigation strategies, this research endeavour seeks to inform policymakers, cybersecurity practitioners, and other stakeholders about the evolving cybersecurity landscape and the imperative of proactive measures to safeguard digital assets and infrastructure. This aims to contribute to the growing body of knowledge on AI-related cybersecurity vulnerabilities and prospects in Bangladesh.

To assess the threat level of AI-based cyber threats in the context of Bangladesh, the paper adopts an exploratory and qualitative research design, focusing on in-depth Key Informant Interviews (KIIs) to investigate the cybersecurity landscape and AI-related threats in Bangladesh. This approach is chosen due to the complexity of the research topic, requiring a deep understanding of participants' perspectives, experiences, and perceptions. By conducting open-ended discussions with key informants, the study aims to explore diverse viewpoints and uncover underlying factors influencing cybersecurity practices. Additionally, relevant literature and case studies are included to provide real-world examples and contextual insights into AI-related threats, enriching the qualitative data and enhancing the exploration of AI-based cyber threats in Bangladesh.

Data collection involves semi-structured Key Informant Interviews (KIIs) with cybersecurity experts, government officials, industry professionals, and other relevant stakeholders in Bangladesh. This format ensures key topics are covered while allowing for in-depth exploration of specific areas of interest. Interview questions are designed to elicit detailed responses, encouraging participants to share their insights, experiences, and recommendations. Special emphasis is placed on gathering insights from AI specialists to understand the technical challenges and potential solutions related to AI-driven cybersecurity threats. This targeted approach ensures the data collected is relevant and informative, providing a solid foundation for analysing the cybersecurity landscape and developing effective mitigation strategies in Bangladesh.

While this discussion endeavours to offer insights into AI-related cybersecurity vulnerabilities in Bangladesh, it is important to acknowledge certain limitations. Firstly, the paper's scope may be constrained by the availability and reliability of data, particularly concerning cybersecurity incidents and AI adoption trends in the country.

Additionally, the research conducted here is not exhaustive in its examination of all possible AI-driven threats and their implications for cybersecurity. Moreover, given the rapidly evolving nature of technology and cybersecurity, the findings of the study may be subject to change over time. Despite these limitations, the paper aims to provide valuable initial insights into the emergent challenges and opportunities at the nexus of AI and cybersecurity in Bangladesh, laying the groundwork for future research and policy interventions in this domain as this technology evolves. With these objectives outlined, the subsequent section on the context and significance of AI-based cyber threats, provides a foundational understanding. This foundational understanding is of the relevance and implications of AI-driven cybersecurity risks, and the scope of the paper involving the sectors that are to be discussed here.

2. Context and Significance of AI-Based Cyber Threats

Despite the rapid integration of artificial intelligence (AI) technologies into various sectors in Bangladesh, the country is confronted with a growing array of cybersecurity vulnerabilities stemming from the adoption of these technologies. The convergence of AI and cybersecurity presents novel challenges that demand attention, particularly in a context where digital infrastructure and regulatory frameworks are still evolving. The problem statement of this research is to comprehensively assess the cybersecurity vulnerabilities posed by AI technologies in Bangladesh and to identify effective strategies for mitigating these risks. This entails understanding the specific threats posed by AI-driven attacks, examining the factors contributing to vulnerability, and proposing targeted interventions to enhance cybersecurity resilience in the country. By addressing this problem, the research aims to inform policymakers, cybersecurity professionals, and other stakeholders about the urgent need to address AI-related cybersecurity challenges and to foster a secure and resilient digital ecosystem in Bangladesh.

The primary research questions guiding this study are: What are the specific cybersecurity vulnerabilities presented by AI technologies in Bangladesh? Additionally, what factors can contribute to the propagation (or the lack thereof) of AI-based cybersecurity vulnerabilities? These questions aim to uncover the unique challenges posed by AI technologies in the context of Bangladesh's cybersecurity landscape and to understand the underlying factors that influence the prevalence of these vulnerabilities.

The objectives of this research are threefold. First, it seeks to analyse the specific cybersecurity vulnerabilities posed by AI technologies in Bangladesh and the factors involved in propagating (or not propagating) these vulnerabilities. Second, it aims to propose targeted mitigation strategies to address AI-related cybersecurity

vulnerabilities in Bangladesh, if applicable. Lastly, the research intends to provide recommendations for policymakers, cybersecurity practitioners, and other stakeholders[5] to enhance cybersecurity resilience in the context of developments in AI technology. These objectives aim not only to identify and understand the current landscape of AI-related cybersecurity threats but also to offer practical solutions and policy guidance to strengthen Bangladesh's defence against such threats.

For the scope of this paper, the discussion focuses on examining cybersecurity vulnerabilities arising from the adoption of artificial intelligence (AI) technologies within the context of Bangladesh. The scope of the study thus encompasses an analysis of specific AI-driven threats, including but not limited to adversarial machine learning, AI-driven phishing attacks, and manipulation of AI algorithms. Additionally, the research aims to investigate the factors contributing to cybersecurity vulnerabilities in Bangladesh, considering socioeconomic, regulatory, and technological dimensions. The study draws upon both qualitative and quantitative data sources to provide a comprehensive understanding of the cybersecurity landscape in the country, with a specific focus on the intersection of AI and cybersecurity. Following this context, section 3 evaluates the current state of cybersecurity in the country, identifying specific vulnerabilities and threats. section 4 describes the qualitative methodology used to assess AI-based cyber threats, and section 5 outlines data collection methods and the importance of expert insights for mitigation strategies. The paper concludes with an emphasis on the need for further research and policy interventions to address these evolving challenges.

This paper holds significant implications for various stakeholders within Bangladesh's digital ecosystem, especially considering that AI technology is still in its early phases of development locally. By exploring the extent of AI-based cyber threats to Bangladesh's cybersecurity infrastructure, the research aims to provide critical insights into the potential impact of emerging technologies on the nation's digital security landscape. Despite AI technology being in its nascent stages within Bangladesh, the study acknowledges the global nature of cybersecurity threats and the potential for external AI-driven attacks to pose significant risks. By examining the specific threats that may emanate from outside the country, the research sheds light on the evolving nature of cybersecurity vulnerabilities and the imperative for proactive measures to safeguard Bangladesh's digital assets.

[5] The stakeholders here also include AI and cybersecurity researchers and academics, healthcare sector representatives, human resources sector stakeholders, the general public and technology users, private sector and businesses, educational institutions, media and awareness campaign organisers who can benefit from what this paper tries to explore.

Furthermore, the study's findings are crucial for local cybersecurity practitioners and professionals. While AI threats may not yet be pervasive within Bangladesh, understanding their potential impact is essential for preparing effective defence strategies. By identifying key risk factors and proposing targeted mitigation measures, the research empowers local cybersecurity teams to anticipate and counteract emerging threats, thereby bolstering the nation's cybersecurity resilience. Additionally, the research serves as a wake-up call for businesses, organisations, and individuals operating within Bangladesh. Even in the early stages of AI development, the potential for external AI-driven attacks to disrupt local operations and compromise sensitive data cannot be overlooked. Implementing the recommended mitigation strategies can help mitigate these risks, ensuring the continued security and stability of Bangladesh's digital infrastructure.

Moreover, the study contributes to academic discourse by providing empirical insights into the evolving cybersecurity landscape. By exploring the threats posed by emerging AI technologies, the research advances scholarly understanding of the intersection between AI and cybersecurity, informing future research directions and policy discussions in this critical area. Therefore, this study's significance lies in its potential to inform policy, empower local cybersecurity practitioners, protect digital assets, and contribute to academic scholarship, ultimately enhancing Bangladesh's resilience against emerging AI-related cybersecurity threats, regardless of their current developmental stage locally.

3. Existing Discussions on Cyber Security in the Context of AI

This section discussed existing literature involving key concepts and research findings relevant to the intersection of artificial intelligence (AI) and cybersecurity, with a specific focus on the context of Bangladesh.

3.1 *Overview of AI in Cybersecurity*

Artificial intelligence (AI) has emerged as a transformative technology with profound implications for cybersecurity. In recent years, AI has been increasingly integrated into cybersecurity practices to enhance threat detection, response, and mitigation capabilities. This section provides an overview of AI's role in cybersecurity, exploring its applications, challenges, and implications for digital security. AI technologies, such as machine learning, natural language processing, and neural networks, enable automated analysis of vast amounts of data to identify patterns, anomalies, and potential threats. In cybersecurity, AI-powered systems can

augment human capabilities by rapidly processing and interpreting data from diverse sources, enabling proactive threat detection and response.[6]

One of the key applications of AI in cybersecurity is in the realm of threat detection and prevention. AI algorithms can analyse network traffic, endpoint behaviour[7], and user activities to identify suspicious patterns indicative of cyber-attacks, such as malware[8] infections, phishing attempts, and insider threats.[9] By leveraging machine learning models trained on large datasets of historical security incidents, AI systems can continuously adapt and evolve to detect emerging threats in real-time.[10] Additionally, AI technologies play a crucial role in automating and optimising cybersecurity workflows.[11] AI-powered tools can streamline routine tasks, such as patch management[12], vulnerability scanning, and incident response, freeing up cybersecurity professionals to focus on more strategic initiatives. Furthermore, AI-driven orchestration and automation platforms enable organisations to orchestrate responses to cyber incidents rapidly,[13] minimising the impact of security breaches.

However, despite its transformative potential, AI also presents challenges and risks in the cybersecurity domain. Adversarial machine learning techniques can be used to evade AI-powered security defences by exploiting vulnerabilities in AI algorithms. Moreover, the proliferation of AI-driven attacks, such as AI-generated phishing emails and deepfake[14] videos, pose new challenges for cybersecurity practitioners. These low-level attacks are particularly relevant for the cyber infrastructure of a country such as Bangladesh with its relatively low overall cyber-awareness.

Previous studies have extensively explored the intersection of artificial intelligence (AI) and cybersecurity, focusing on the vulnerabilities and risks posed by

[6] Ivano Lauriola, Alberto Lavelli and Fabio Aiolli, "An introduction to deep learning in natural language processing: Models, techniques, and tools," *Neurocomputing* 470, (2022): 443–456.
[7] I.e., the results that take place within a user's device during any online activity, such as a webpage showing up on a screen, or a monetary transaction being confirmed during online payment.
[8] I.e., malicious software programmed to harm a user's electronic device or compromise a user's data.
[9] Christoffer Sjöblom, "Artificial Intelligence in Cybersecurity and Network security," Master's Thesis (Åbo Akademi University: 2021), https://www.doria.fi/handle/10024/181168
[10] Sakthiswaran Rangaraju, "AI Sentry: Reinventing Cybersecurity Through Intelligent Threat Detection," *EPH-International Journal of Science and Engineering* 9, no. 3 (2023): 30–35.
[11] Iqbal H. Sarker, "Ai-based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent And Smart Systems," *SN Computer Science* 3, no. 2 (2022): 158.
[12] I.e., updating existing software or cyber-infrastructure to be able to withstand attacks from newly made malicious software (i.e., malware).
[13] Sukhpal Singh Gill *et al*., "AI for next generation computing: Emerging trends and future directions," *Internet of Things* 19 (2022): 100514.
[14] Software that can be used to make artificial identical replicas of people's likeness in image, audio, or video form.

AI technologies in digital security frameworks. These studies have contributed valuable insights into the emerging threats and challenges associated with AI-driven cyber-attacks, as well as potential mitigation strategies to enhance cybersecurity resilience.

Researchers have investigated various AI-related cybersecurity vulnerabilities, including adversarial machine learning, AI-driven phishing attacks, and manipulation of AI algorithms. Adversarial machine learning techniques exploit vulnerabilities in AI models by injecting malicious inputs or perturbation[15], leading to misclassification or manipulation of AI-based systems.[16] Studies have demonstrated the susceptibility of AI algorithms, such as image classifiers and malware detectors, to adversarial attacks, highlighting the need for robust defences against adversarial manipulation.[17] Studies regarding the capabilities of cyber criminals show that the tech level of criminals executing cyber-attacks rely more on social engineering to gain an edge in their successful execution of attacks over using cutting edge technology–technology that they often do not have access to.[18]

Moreover, AI-driven phishing attacks leverage natural language processing and generative models to craft sophisticated phishing emails that evade traditional detection mechanisms. These attacks exploit human vulnerabilities by impersonating trusted entities or generating convincing social engineering messages, increasing the likelihood of successful phishing attempts. Previous research has examined the effectiveness of AI-based phishing detection techniques and proposed countermeasures to mitigate the impact of AI-driven phishing attacks on organisational security. Additionally, studies have investigated the manipulation of AI algorithms to subvert their intended functionality or decision-making processes. Attackers can exploit vulnerabilities in AI systems to manipulate outcomes, evade detection, or bypass security controls, posing significant risks to digital infrastructure and sensitive data.[19] Research efforts have explored techniques for detecting and mitigating AI algorithm manipulation, such as robustness testing, anomaly detection, and adversarial training.

---

[15] Perturbations are jargon codes intended to muddy a database, which can result in the database slowly becoming corrupted with unreliable information and then turning unusable in the process.

[16] Ling Huang *et al.*, "Adversarial machine learning," in *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, (2011) 43–58.

[17] Shruti Patil *et al.*, "Improving the robustness of ai-based malware detection using adversarial machine learning," *Algorithms* 14, no. 10 (2021): 297.

[18] E. Rutger Leukfeldt, Edward R. Kleemans and Wouter P. Stol, "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists," *Crime, Law and Social Change 67* (2017): 21–37.

[19] Miles Brundage et al., 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation' (arXiv, 2018), https://doi.org/10.48550/ARXIV.1802.07228

3.2 *Current State of Cybersecurity in Bangladesh*

Nadeem et al.[20] conducted an in-depth survey on the awareness of cybercrime among the people of Bangladesh. The abstract underscores the pervasive influence of digital devices and the internet in everyday life, emphasising the transformative impact of technology on communication, education, and information access. The study highlights the emergence of cybercrime as a pressing issue, particularly in developing countries like Bangladesh. Despite the convenience afforded by digital technologies, the study reveals a patchy awareness level[21] of cybercrime among the general population, indicating a lack of understanding of standard cybersecurity practices.

Connecting the findings from the study by Nadeem et al., we see a cohesive narrative emerging regarding the state of cybersecurity awareness in Bangladesh from another study from Mamun, Ibrahim, and Mostofa.[22] Both studies underscore the increasing reliance on technology in Bangladesh, which has led to a significant rise in cybersecurity risks and threats. Mamun, Ibrahim, and Mostofa highlight the proliferation of cyber assaults and the emergence of cyber wars as major concerns, indicating a growing recognition of the severity of cybersecurity challenges in the country. Similarly, Nadeem et al. emphasise the prevalence of cybercrime and the urgent need for improved cybersecurity awareness among the population.

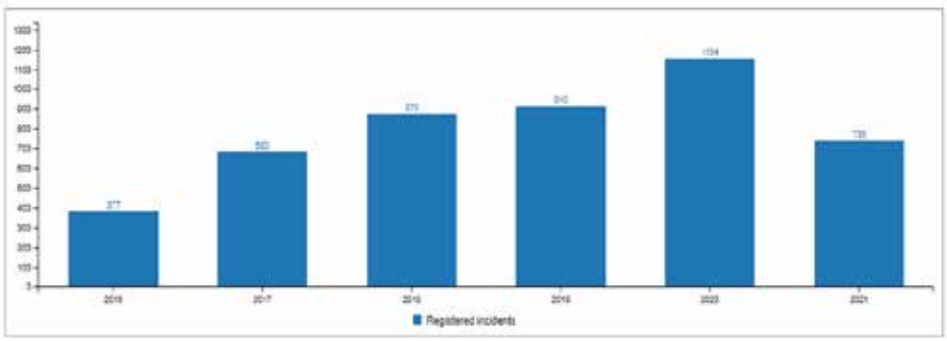
Despite the efforts of government and non-government actors to raise awareness of cybersecurity issues, both studies find troubling levels of comprehension deficiency among Bangladeshi citizens. Mamun, Ibrahim, and Mostofa note a substantial lack of awareness of cybersecurity mechanisms and regulations, while Nadeem et al. highlight a low awareness level and unsatisfactory understanding of standard cybersecurity practices among the general populace. Moreover, both studies highlight the lack of proactive response from associated organisations and the government in addressing cybercrime-related issues. Mamun, Ibrahim, and Mostofa advocate for a major change in cybersecurity policies and procedures, emphasising the need for supervision and restructuring over time. Similarly, Nadeem et al. call for

[20] Nadeem Ahmed *et al.*, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, (2017): 788–791.
[21] Also see Nadeem Ahmed *et al.*, "Demographic factors of cybersecurity awareness in Bangladesh," in *2019 5th International Conference on Advances in Electrical Engineering (ICAEE),* (IEEE, 2019): 685–690.
[22] Abdullah Al Mamun, Jamaludin Bin Ibrahim, and Sk Mamun Mostofa, "Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies," *Int. J. Comp. Sci. Informat. Technol. Res* 9 (2021): 88–94.

the implementation of a proper guideline for cybersecurity and stress the importance of timely updates to combat evolving cyber threats.

Moreover, Chowdhury et al.[23] identify various challenges to cybersecurity in Bangladesh, including the lack of legal frameworks, inefficient technical institutions, and insufficient

Figure 1: Cyber Incidents in Bangladesh Per Year



Source: Rahaman, "Recent Advancement of Cyber Security"

organisational capacity building. This resonates with the observations made by both Mamun, Ibrahim, and Mostofa, and Nadeem et al., regarding the patchy awareness level of cybersecurity among citizens and the inadequate response from associated organisations and the government. In proposing policy options to address these challenges, Chowdhury et al. echo the calls for major changes in cybersecurity policies and procedures put forth by Mamun, Ibrahim, and Mostofa, and Nadeem et al. By advocating for the development of a digitally connected, safe, and secure Bangladesh by 2030, Chowdhury *et al*. reinforce the urgent need for proactive measures to strengthen cybersecurity governance, enhance technical capabilities, and foster cooperation mechanisms among stakeholders.

Cyberattacks have been on the rise in Bangladesh over the years, posing significant challenges for individuals, corporations, and governmental entities. The increasing prevalence of cyber threats, including ransomware, phishing attacks, malware infections, and other cybersecurity risks, has underscored the urgent need for enhanced cybersecurity measures in the country. The above figure shows how cyberattacks have become more and more prevalent in Bangladesh over the years.

[23] Tamjidul Haque Chowdhury *et al.*, "Cybersecurity Challenges and Policy Options for Bangladesh," in *2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*, (2021): 472–476.

Data from the tribunal in Bangladesh reveal a concerning trend in cybercrime incidents, with the number of complaints steadily increasing from 33 in 2014 to 1,189 in 2019. This significant rise in reported cybercrime cases reflects the growing sophistication and prevalence of cyberattacks targeting individuals, businesses, and government institutions. Furthermore, the onset of the COVID-19 pandemic in 2020 further exacerbated cyber threats, with 1,128 cases filed during that year alone. The pandemic-induced shift towards remote work and increased reliance on digital technologies created new opportunities for cybercriminals to exploit vulnerabilities and launch cyberattacks against unsuspecting victims.[24]

Ransomware[25] attacks, in particular, have emerged as a major concern for organisations in Bangladesh.[26] Ransomware is a type of malicious software that encrypts a user's data and demands payment in exchange for restoring access. These attacks not only disrupt operations but also pose significant financial and reputational risks for affected organisations. The inability to access critical data can cripple business operations, leading to financial losses and reputational damage.

The proliferation of Internet of Things (IoT) devices[27] Further amplifies the cyber threat landscape in Bangladesh. As the number of IoT devices continues to grow exponentially, so does the potential risk of cyberattacks targeting these devices. Compromised IoT devices can be used as entry points for hackers to gain access to sensitive data or launch distributed denial-of-service (DDoS) attacks, posing significant security and privacy risks for users.

Research on cybersecurity in Bangladesh has gained a small amount of traction in recent years, reflecting at least some of the growing recognition of how important digital security is for the country's socio-economic development. Existing studies have explored various aspects of cybersecurity, including threat landscapes, regulatory frameworks, awareness levels, and policy interventions.

Studies examining the threat landscapes in Bangladesh have identified a range of cybersecurity challenges, including phishing attacks, malware infections, and data

[24] Rahaman, "Recent Advancement of Cyber Security".

[25] Ransomware is a form of malware used to target an individual's sensitive data on a personal device and encrypt them. The attacker who sent the malware can then ask for ransom in order to offer to decrypt the files and return the user's data.

[26] Ransomware prevalence Further elaborated in, Samantha Haque and Touhid Bhuiyan, "Rise of Ransomware and the Readiness of Bangladesh," in *International Conference on Latest Trends in Engineering and Technology* 10. (2017).

[27] I.e., devices that are always connected to the internet, and depend on that 'always on connection' to function properly. Examples include security cameras, sensors in industrial complexes, smart home devices, and electric cars.

breaches. These studies highlight the vulnerability of Bangladesh's digital infrastructure to cyber threats and underscore the need for robust cybersecurity measures to mitigate risks effectively.[28] Moreover, research on regulatory frameworks for cybersecurity in Bangladesh has analysed the adequacy of existing laws and policies in addressing emerging cyber threats. Scholars have assessed the strengths and weaknesses of regulatory frameworks governing data protection, cybercrime prevention, and incident response, providing insights into areas for improvement.

Additionally, as previously mentioned above, studies on cybersecurity awareness in Bangladesh have investigated the level of awareness among different stakeholders, including government agencies, businesses, and the public.[29] These studies have identified gaps in understanding cybersecurity risks and best practices, emphasising the importance of education and training programs to enhance awareness and build a cyber-resilient society. Furthermore, research on policy interventions for cybersecurity in Bangladesh has proposed recommendations for strengthening cybersecurity governance, enhancing technical capabilities, and fostering collaboration among stakeholders.[30] Scholars have advocated for the development of comprehensive cybersecurity strategies that integrate legal, technical, and institutional measures to address evolving cyber threats effectively.

3.3 *Cybersecurity Vulnerabilities in Bangladesh*

Cybersecurity vulnerabilities in Bangladesh represent a complex and evolving landscape shaped by various socio-economic, technological, and regulatory factors. This section examines the specific vulnerabilities that expose Bangladesh's digital infrastructure to cyber threats and highlights key areas of concern. One of the primary cybersecurity vulnerabilities in Bangladesh is the prevalence of phishing attacks and social engineering scams. Cybercriminals often target individuals and organisations through deceptive emails, messages, or phone calls, aiming to steal sensitive information or perpetrate financial fraud. The lack of awareness among users and insufficient cybersecurity training exacerbates the effectiveness of these attacks, making phishing a significant threat to Bangladesh's cybersecurity posture. In that

[28] Nahid Joveda, Md Tarek Khan and Abhijit Pathak, "Cyber laundering: a threat to banking industries in Bangladesh: in quest of effective legal framework and cyber security of financial information," *International Journal of Economics and Finance* 11, no. 10 (2019): 54–65.
[29] Chowdhury *et al.*, "Cybersecurity Challenges and Policy Options".
[30] M. M. Rahaman, "Recent advancement of cyber security: Challenges and future trends in Bangladesh," *Saudi Journal of Engineering and Technology* 7, no. 6 (2022): 278–289.

respect, the study by Joveda, Khan, and Pathak[31] sheds light on the emerging threat of cyber laundering in the banking industry of Bangladesh, highlighting the abuse of information technology to conceal the original source and illegally transfer money. This phenomenon underscores the inherent vulnerabilities in Bangladesh's banking infrastructure, particularly concerning cybersecurity and financial information protection. Cyber laundering[32] poses a significant risk to the integrity and stability of Bangladesh's banking sector, with potential implications for the local economy and global financial systems. The study's examination of launderers' typology of crimes, both potential and real, emphasises the need for proactive measures to detect and prevent cyber laundering activities. The study also calls attention to the inadequacies of existing national control mechanisms in addressing the challenges of money laundering in banks. This aligns with the broader discussion on cybersecurity vulnerabilities in Bangladesh, which highlights weaknesses in regulatory frameworks, organisational capabilities, and technical infrastructure.

Moreover, the proliferation of malware infections poses a considerable risk to Bangladesh's digital ecosystem. Malware variants, such as ransomware, spyware, and botnets, exploit vulnerabilities in software and systems to compromise data integrity, disrupt operations, and extort financial gains. Weaknesses in software patching practices and inadequate cybersecurity hygiene contribute to the susceptibility of Bangladesh's digital infrastructure to malware threats. Furthermore, inadequate data protection measures and insufficient regulatory oversight contribute to cybersecurity vulnerabilities in Bangladesh. The lack of comprehensive data protection laws and enforcement mechanisms leaves personal and sensitive data exposed to unauthorised access, misuse, or theft. Cybercriminals exploit these vulnerabilities to compromise privacy, commit identity theft, and perpetrate cyber espionage, posing significant risks to individuals, businesses, and government entities.

An illustrative case study within Bangladesh's cybersecurity landscape involves a significant money laundering operation that underscored vulnerabilities within the financial sector. Although AI was not directly implicated in this instance, examining this case offers insights into the potential intersection of cyber vulnerabilities and artificial intelligence (AI) and sheds light on how AI could potentially exacerbate such risks. In this case, cybercriminals exploited weaknesses in banking security protocols and regulatory oversight to conceal illicit funds' origin and destination, misplacing over US$81 million from the bank reserves. [33] While AI was not employed in this

[31] Joveda, Khan, and Pathak, "Cyber laundering".
[32] Cyber-laundering is the act of laundering money through digital channels.
[33] Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," *Wired*, 17 May, 2016, https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

specific attack, it is pertinent to recognise the potential role AI could play in facilitating and amplifying similar cybercrimes. AI-powered tools could streamline and automate various stages of the money laundering process, from identity theft and fraud detection evasion to money mule recruitment and transaction concealment. The sophistication and scale of this operation underscore the potential for AI-driven techniques to enhance cybercriminals' capabilities in orchestrating complex financial crimes. Nevertheless, this encompasses nearly all the relevant literature that explores cybersecurity threats in a systematic manner that can be used to draw conclusions on current developments regarding the country's vulnerability to such attacks. This leaves ample room for further studies towards assessing the cybersecurity capabilities of Bangladesh, especially when it comes to AI-based cyber threats, an area without any significant studies in Bangladesh's context. This paper attempts to add to that gap.

The evolving landscape of cyber threats highlights the urgency of integrating AI into cybersecurity strategies to bolster defences and mitigate risks effectively. However, it is essential to acknowledge that AI can also introduce new challenges and vulnerabilities. AI-powered algorithms could be exploited by malicious actors to bypass security measures, evade detection, and automate attacks at scale. For example, AI algorithms could be trained to generate convincing phishing emails, manipulate financial transactions, or impersonate legitimate users, making it increasingly difficult for traditional security measures to detect and prevent cyber threats. By contextualising this case study within the broader discussion of AI-driven cyber threats, the paper underscores the importance of proactive measures to mitigate risks and safeguard against financial crimes. While AI presents opportunities for enhancing cybersecurity defences, it also necessitates robust safeguards, regulations, and ethical considerations to prevent its misuse and exploitation by cybercriminals.

As rapid digitisation takes place within critical infrastructure sectors, such as finance, healthcare, and transportation, new cybersecurity vulnerabilities are introduced. The interconnected nature of digital systems increases the attack surface and amplifies the impact of cyberattacks on essential services and national security. Weaknesses in cybersecurity preparedness, incident response capabilities, and cross-sector coordination further exacerbate the vulnerabilities of Bangladesh's critical infrastructure to cyber threats.

3.4 *Overview of AI-related Cybersecurity Threats in the Context of Bangladesh*

One of the primary AI-related cybersecurity threats is the emergence of adversarial machine learning techniques. Adversarial attacks exploit vulnerabilities in

AI models by injecting malicious inputs or perturbations, leading to misclassification or manipulation of AI-powered systems. These attacks undermine the integrity and reliability of AI-based security defences, enabling attackers to evade detection and compromise sensitive data or systems.

The type of cyberattack that may concern a country like Bangladesh the most is the proliferation of AI-driven phishing attacks. Attackers leverage AI algorithms to craft sophisticated phishing emails or messages that mimic legitimate communication, increasing the likelihood of successful social engineering attacks. AI-powered phishing techniques enable attackers to personalise and contextualise phishing attempts, making them more convincing and difficult to detect using traditional security measures. This has the significant risk of making previously sophisticated cyber-attacks more accessible to the average miscreant and make organising large-scale attacks more feasible for smaller hacking communities. Despite ongoing parallels in research in using AI-based detection mechanism to reliably block phishing attacks[34], the abovementioned social-engineering attacks pose a threat to the cyber infrastructure of Bangladesh.

In the context of Bangladesh, several specific vulnerabilities exacerbate the cybersecurity landscape, presenting unique challenges for digital security practitioners and policymakers. One prominent vulnerability stems from the rapid digitisation of critical infrastructure sectors, such as finance, healthcare, and transportation. While digital transformation offers numerous benefits, including increased efficiency and accessibility, it also expands the attack surface and introduces new cyber threats. Weaknesses in cybersecurity preparedness and incident response capabilities within these sectors expose them to risks of cyber-attacks, data breaches, and service disruptions, with potentially significant implications for national security and public safety.

Additionally, the proliferation of mobile and internet-based technologies in Bangladesh presents another vulnerability, particularly concerning the security of personal and financial data. The widespread adoption of mobile banking, e-commerce platforms, and digital payment systems has facilitated greater connectivity and convenience for users but has also heightened the risks of cyber threats such as phishing attacks, malware infections, and identity theft.[35] Weaknesses in mobile device security, insufficient cybersecurity awareness among users, and limited

[34] Meraj Farheen Ansari, Pawan Kumar Sharma and Bibhu Dash, "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training," *International Journal of Smart Sensor and Adhoc Network* 3, no. 3 (2022): 61–72.
[35] Rahaman, "Recent Advancement of Cyber Security".

regulatory oversight contribute to the susceptibility of individuals and organisations to cyber-attacks, compromising their privacy, financial security, and digital identity.

Furthermore, the lack of comprehensive cybersecurity regulations and enforcement mechanisms in Bangladesh poses a significant vulnerability to cyber threats. While efforts have been made to develop cybersecurity policies and initiatives, gaps remain in regulatory frameworks governing data protection, cybercrime prevention, and incident response. The absence of robust legal frameworks and enforcement mechanisms hampers efforts to combat cybercrime effectively, leaving individuals, businesses, and government entities vulnerable to cyber-attacks and financial fraud. The shortage of skilled cybersecurity professionals and inadequate investment in cybersecurity education and training exacerbate vulnerabilities in Bangladesh's digital ecosystem. The demand for cybersecurity expertise exceeds the supply of qualified professionals, limiting the capacity of organisations to implement effective cybersecurity measures and respond to emerging threats. Insufficient cybersecurity awareness and training programs further compound the problem, leaving users and organisations ill-equipped to recognise and mitigate cyber risks effectively.

4. Assessment of Threat Level of AI-Based Cyber Threats: A Discussion

Findings show a stark contrast to the possibilities of AI-based Cyber threats in Bangladesh. The areas of personal data security, health sector, and human resources sector have been discussed by key informants regarding their potential for being vulnerable to AI-based cyber threats. The findings start with the level of existing threats from AI-based cyber threats in general before moving on to the specific sectors which are a part of this paper. A Security Officer closely involved with the cyber security and intelligence in the financial sector has posited that the threat of cyber-attacks of any sort from technologies dependent on AI is particularly low to non-existent. He elaborated with,

> "AI-based technology is relatively new and needs a very complex understanding of programming to execute at a general level with very expensive hardware. Cyber criminals do not have the tech level at the moment to execute that, and at the same time be as cost-effective with their old reliable methods."[36]

This sets the backdrop of the resource-intensive nature of this technology, as executing complex operations of cyber-attacks with the help of this technology

[36] Interviewee A (a Security Officer closely involved with the cyber security and intelligence in the financial sector, based in Dhaka City), taken in Dhaka on April 2024.

requires specialised expertise not often available to cyber attackers. The literature also shows that despite cyber criminals having a higher skill level than less technical 'ordinary attackers'[37], their resources are generally lacking in terms of being at the cutting edge of technology. Rather, they rely on aspects of social engineering that rely on establishing direct communication with the victims to gather access information[38], rather than the latest technological developments.[39]

Before moving on to the specific areas tackled by this study, a professor closely working with AI-based technology and developments in machine learning has argued that this technology is not easily utilised in executing cyber-attacks due to how focused its development process is. He elaborates his argument with,

> "AI models are not being trained to execute cyber-attacks, since it is something companies actually training them are not interested in, and is something that cyber criminals have not developed themselves. It is far more cumbersome at the moment even to attempt it than following established methods that continue to greatly profit these criminal networks already. The extensive resource to build up AI-models to target continuously developing security infrastructures is not nearly as efficient for such groups yet."[40]

These two outputs set the backdrop of the current low threat-level from AI-based cyber threats in Bangladesh. However, the specifics of the targeted areas discussed in this study should be explored to fully understand the reasons behind this. At the level of personal security, a Cyber Security Response Specialist elaborated on how AI-based phishing attacks–a key form of AI-based cyber threat in the personal data security sphere, is not feasible in Bangladesh's context to any significant degree. He elaborated with,

> "AI-based phishing is email-based, involving forging believable documents. These will not work here (i.e., in Bangladesh). People using emails will not be baited to these attacks, to begin with… attacks involving direct calls are far more effective and much easier to execute than using such sophisticated AI-tech to launch such attacks. The knowledge has not trickled down to such people here yet."

His elaboration extends to how the low-tech methods used by cyber criminals (i.e., methods involving direct calls, alongside old methods involving long-practiced

[37] Jim AM Schiks, Steve GA van de Weijer, and E. Rutger Leukfeldt, "High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals," *Computers in Human Behavior* 126 (2022): 106985.

[38] I.e., information that helps cyber attackers get access to sensitive data and thus commit their crimes successfully.

[39] Leukfeldt, Kleemans, and Stol, "A typology of cybercriminal networks".

[40] Interviewee B (a Cyber Security Response Specialist based in Dhaka City), taken in Dhaka on April 2024.

website-based scam attacks etc.), are low-cost methods. These low-cost methods require a lowlevel of education and resources in comparison to the expensive technology and high level of skill required to not only train on but also execute AI-based phishing attempts. He further solidified his argument by adding that such pathways are not even feasible at the higher level of cyberattacks due to the evolving nature of security infrastructures. This greatly lowers the possibility of AI-based cyberattacks in the personal data security sphere.

As for adversarial machine learning risks in the fields of health diagnostics and human resources, key informants have elaborated on how the very early phase and testing in both of these fields render such risks insignificant. One expert on AI models posited that,

> "AI models are only being tested in the healthcare division as a form of learning how these can be applied at a general level. These models will not be considered towards seriously supplementing any real professional in the near future."[41]

He further emphasised how the small scope of these testing experiments decreases the risks of adversarial machine learning. "And if such somehow attempts took place," he posited, "then the results will already be faulty, making these (AI) models unfit for any practical use, let alone in healthcare."[42] This sets the ground for how little is being considered in implementing AI-models in healthcare, to diagnose diseases and suggest remedies.

In the field of Human Resources (HR), models are being tested, but detailed information has been scarce. A key informant has given his insights in this area,

> "AI models to enhance HR department's work to hire and recruit workers are only being proposed at the moment. This is unlikely to be significant progress in this area in Bangladesh since people here will not take the news of being hired by a machine kindly, frankly speaking."[43]

He substantiated his words with how in Bangladesh, with a lowering overall employment rate, the last thing a company operating in its borders wants is being labelled as a company resorting to replacing its workforce with AI models and using it to hire more personnel, which would greatly downgrade a company's image.

[41] Interviewee C (a Professor specialising in machine learning and Large Language Models (LLMs) and their applications, based in Dhaka City), taken in Dhaka on May 2024.
[42] Ibid.
[43] Interviewees A and D (a Professor of cyber security specialising in machine learning and Large Language Models (LLMs) and their applications, based in Dhaka City), taken in Dhaka on April 2024.

However, he concluded by mentioning how the actual developments further in the future can change depending on the progress made in the technology.

Based on the above discussion, the threat assessment of AI-based cyber threats in Bangladesh reveals several factors contributing to the current low level of risk. According to a Security Officer involved in cybersecurity and intelligence within the financial sector, the likelihood of cyberattacks utilizing AI technologies is minimal to non-existent. He argues that AI-based technologies are still in their infancy and require advanced programming skills and expensive hardware, making them less accessible and cost-effective for cybercriminals. Instead, these criminals continue to rely on traditional methods, such as social engineering, which involve direct communication with victims to extract sensitive information. The literature supports this view, indicating that while cybercriminals may possess higher technical skills than ordinary attackers, they typically lack the resources to employ cutting-edge technologies, instead opting for tried-and-true techniques.

Additionally, a professor specializing in AI and machine learning highlights that AI models are not designed to execute cyberattacks, as their development is focused on other applications. Companies training AI models are not interested in creating tools for cybercriminals, and such criminals have not developed the technology themselves. He notes that building AI models to target ever-evolving security infrastructures is inefficient and cumbersome compared to established methods that continue to yield substantial profits for criminal networks. This underscores the resource-intensive nature of developing and deploying AI for cyberattacks, further explaining the current low threat level from AI-based cyber threats in Bangladesh.

The study then examines the specific areas of personal data security, healthcare, and human resources to understand the nuanced reasons behind the low threat level. In terms of personal security, a Cyber Security Response Specialist explains that AI-based phishing attacks are not feasible in Bangladesh. AI-based phishing typically involves sophisticated email forgeries, but in Bangladesh, email-based attacks are less effective, and cybercriminals find direct calls and traditional website scams more practical and cost-effective. These methods require minimal education and resources compared to the expensive technology and high skill level needed for AI-based phishing, making the latter less appealing to local cybercriminals.

Regarding adversarial machine learning risks in healthcare and human resources, key informants note that AI models in these sectors are still in early testing phases. An expert on AI models in healthcare mentions that these models are currently being tested to explore their potential applications and are not yet ready to replace

professionals. The limited scope of these tests reduces the risk of adversarial attacks, and any such attempts would likely result in faulty outputs, rendering the AI models impractical for real-world use. This early stage of AI implementation in healthcare suggests minimal risk of adversarial machine learning attacks.

In the human resources sector, AI models have been proposed to enhance hiring and recruitment processes, but their adoption is still in the proposal stage. A key informant highlights that there is resistance to the idea of being hired by a machine, given the cultural and economic context of Bangladesh, where unemployment rates are a concern. Companies fear being perceived as replacing human workers with AI, which could damage their reputation. This cultural resistance and the nascent stage of AI implementation in HR further contribute to the low risk of AI-based cyber threats in this sector.

Thus, the high resource requirements, lack of technical capability among cybercriminals, and the nascent stage of AI adoption in critical sectors collectively explain why AI-based cyberattacks are not a significant concern at present. However, continuous monitoring and adaptive strategies are essential as AI technologies evolve and their implementation becomes more widespread.

5. Assessment of Threat Level of AI-Based Cyber Threats: Way Forward

Regarding future directions that need to be taken into account for possible new developments in AI-based cyber threats, key informants have supported the notion of continuously emphasising increased cyber awareness and a focus on cyber literacy across the general public.[44] This emphasis on education and awareness is seen as a crucial component in the fight against sophisticated cyber threats, particularly as AI technologies become more advanced and accessible. One key aspect of this approach is the development and implementation of comprehensive cyber literacy programs. These programmes should be designed to educate individuals about the nature of AI-based cyber threats, how they can recognise potential attacks, and what steps they can take to protect themselves. Such education should start at an early age, with cyber literacy being integrated into school curricula. By teaching students about the importance of cybersecurity from a young age, they will grow up with a better understanding of the risks and how to mitigate them.[45]

Additionally, key informants have posited that there should be ongoing public awareness campaigns aimed at adults. These campaigns can use various media

[44] Nadeem et al., "Cybersecurity awareness survey".
[45] Nadeem et al., "Cybersecurity awareness survey".

channels, including social media, television, radio, and print media, to reach a broad audience.[46] The goal is to keep the public informed about the latest developments in AI-based cyber threats when they arise, and provide practical advice on how to stay safe online. These campaigns can include tips on recognising phishing emails, the importance of strong passwords, and how to secure personal devices.

Literature further supports workshops and training sessions in increasing cyber literacy. Employers, community centres, and educational institutions can organise these sessions to provide hands-on experience in dealing with cyber threats. These sessions can cover a range of topics, from basic internet safety to more advanced topics like identifying AI-generated content and understanding the mechanics of AI-based attacks. However, as for how policies should be implemented at the government level, the low-level of threats posed by this specific type of technology required further scrutiny and exploration to better assess policy requirements. The intention of the key informants to remain anonymous during the data collection process does dampen these initial findings somewhat. However, it is felt that the existing data (or in some cases, a lack thereof) regarding AI-based cyber threats itself backs up these findings.

Therefore, given the current state of AI-based cyber threats and the evolving nature of these technologies, it is essential to adopt a 'wait and see' approach while ongoing research and monitoring continue. At present, the landscape of AI-driven cybersecurity threats remains dynamic and unpredictable, and this requires a cautious stance as a result. This approach allows for the accumulation of more data and insights, enabling a more informed assessment of emerging risks and the effectiveness of preventative measures. To clarify further, the recommendation reached here involves maintaining a cautious yet proactive stance by continuously gathering intelligence on AI-driven threats, refining response strategies, and prioritising adaptive cyber literacy initiatives. As advancements in AI technology and corresponding cyber threats unfold, maintaining flexibility in response strategies and continuously updating cyber literacy initiatives will be crucial in mitigating potential risks. In the interim, stakeholders must remain vigilant and proactive, ensuring that educational and awareness efforts are adaptable to the changing threat environment.

6. Conclusion

This paper has provided a comprehensive assessment of the current threat level posed by AI-based cyber threats in Bangladesh, focusing on personal data security,

[46] Nadeem et al., "Demographic factors of cybersecurity awareness"; Kaushik Sarker *et al.*, "A comparative analysis of the cyber security strategy of Bangladesh," *arXiv preprint* (2019): 1905.00299.

the health sector, and human resources. The findings reveal that the threat from AI-based cyber-attacks in Bangladesh is currently low. This is primarily due to the complex nature of AI technology, which requires advanced programming skills and expensive hardware that are not readily accessible to most cybercriminals. Instead, cybercriminals continue to rely on traditional methods, such as social engineering and direct communication with victims, which are more cost-effective and do not require sophisticated technology.

In the realm of personal data security, AI-based phishing attacks are not a significant threat in Bangladesh. The low-tech methods of direct calls and traditional website scams are more prevalent and practical for cybercriminals in this context. These methods are less resource-intensive and do not require the high level of skill needed for AI-based phishing. In the health sector, AI models are still in the early testing phases, primarily being explored for their potential applications. This limited scope of testing reduces the risk of adversarial machine learning attacks. Even if such attacks were attempted, the current state of AI models would likely produce faulty results, rendering them impractical for real-world use. Similarly, in the human resources sector, AI models for enhancing hiring and recruitment processes are still in the proposal stage. There is significant cultural resistance to the idea of being hired by a machine, particularly given the economic context of Bangladesh, where unemployment rates are a concern. Companies are wary of being perceived as replacing human workers with AI, which could damage their reputation. This cultural resistance, coupled with the early stage of AI implementation, further contributes to the low risk of AI-based cyber threats in this sector.

Moving forward, it is crucial to emphasise continuous cyber awareness and literacy across the general public. Educational programs and public awareness campaigns should be developed to educate individuals about AI-based cyber threats and how to protect themselves. These initiatives should start at an early age and be integrated into school curricula while also targeting adults through various media channels. Workshops and training sessions can provide hands-on experience in dealing with cyber threats, enhancing overall cyber literacy.

Government policies should also be scrutinised and adapted to address the evolving landscape of AI-based cyber threats. While the current threat level is low, it is essential to remain vigilant and proactive in developing strategies to mitigate potential future risks. By fostering a culture of cyber awareness and literacy and by implementing robust policies, Bangladesh can build a resilient defence against the growing challenges posed by AI-based cyber threats.