Managing Escalating Cyber Threats: Perspectives and Policy Insights for Bangladesh

Mohammad Sayduzzaman[1]; Sadia Sazzad[1]; Muaz Rahman[1]; Tawhidur Rahman[2]; and Mohammad Kawsar Uddin[3]
[1]Department of CSE, National Institute of Textile Engineering and Research (NITER),
Constituent Institute of the University of Dhaka, Savar, Dhaka-1350
[2]Digital Security & Digital Diplomacy, Agargaon, Dhaka-1207
[3]Technology Media Guild Bangladesh (TMGB), Mirpur DOHS, Dhaka-1216

Abstract:- As Bangladesh rapidly adopts digital technologies, the country faces escalating cybersecurity threats that can undermine economic development and national security. This paper provides an up-to-date analysis of Bangladesh's cybersecurity landscape, including emerging risks from sophisticated attacks, data breaches, and misinformation campaigns. It examines the regulatory frameworks governing cyberspace and key technologies like artificial intelligence, considering national policies as well as regional and global perspectives. The paper highlights innovative responses to cyber challenges, such as public-private partnerships (PPP), cyber security training programs, and the use of AI for threat detection. However, substantial gaps remain in Bangladesh's cyber defenses. The paper argues for a comprehensive, multi-stakeholder approach to cybersecurity capacity building. Specific recommendations include increasing investments in cyberinfrastructure, expanding cybersecurity education and training, developing effective legal frameworks, and fostering national and international cooperation. Adopting these coordinated strategies can help Bangladesh harness the benefits of digital transformation while safeguarding against intensifying cyber threats. We use OSINT and WebINT to justify our technical analysis.

Keywords:- *Cybersecurity, Bangladesh, Regulation, Artificial Intelligence, State-of-the-Art Responses, Case Studies, CIIO.*

I. INTRODUCTION

The spread of digital technology in a more linked world has not only created unprecedented prospects for creativity and economic progress but has also given rise to a new frontier of global security threats. Our susceptibility to cyber-attacks grows in parallel with our reliance on digital infrastructure. These dangers, which range from sophisticated state-sponsored attacks to criminal businesses, have become a top priority for administrations, organizations, and individuals all around the world. In the twenty-first century, the rapid advancement of information and communication technology has fueled a globalized world heavily dependent on the internet, telecommunications, and digital infrastructure [1], [2].

With this increased connectivity, the threat landscape of cybersecurity has become a pressing concern for nations world-wide. Bangladesh, like many other countries, is confronted with significant challenges in safeguarding its cyberspace from malicious activities and ensuring the security of sensitive data. Significant progress in information and communication technology (ICT) around the world has brought about a corresponding increase in the potential for cybercrime, even in developed and developing countries like Bangladesh [3]. Investigating and prosecuting cybercrimes pose significant challenges for sovereign states in borderless cyberspace [4], [5]. Cybersecurity, as a concept, is ambiguous and subjective, with its definition evolving over time. Bangladesh has made notable advancements in facilitating greater online access for its people and businesses, enabling them to leverage data, digital technologies, and global connectivity [6], [7]. The country boasts the second-largest group of global gig workers, with approximately 15 percent, engaged in creative and multimedia work, generating an estimated annual income of USD 500 million, according to Bangladesh's ICT ministry [7]. The expansion of internet-based activities has also given rise to concerns regarding software protection, curbing cyber-crimes, safeguarding intellectual property rights, enforcing e-commerce rights and liabilities, and ensuring data protection [4], [8], [9]. While the policymakers of Bangladesh have exercised various legal and pragmatic measures to address cybersecurity threats in recent years, there is still a need for further action to ensure comprehensive cybersecurity. Additionally, the involvement of political interests and violations of human rights under the guidance of cyber security legislation has raised ethical concerns [4], [10]. Table I describes the common abbreviations used in this paper.

Table 1 Describes the Common Abbreviations
Used in this Paper.

	List of Common Abbreviations with Description.
Keys	Description
AI	Artificial Intelligence
AFD	Armed Forces Division
BAF	Bangladesh Air Force
BCC	Bangladesh Computer Council
BPDB	Bangladesh Power Development Board
BSCL	Bangladesh Satellite Company Limited
BSEC	Bangladesh Satellite and Exchange Commission
BTRC	Bangladesh Telecommunication Regulatory Commission

CDBL	Central Depository Bangladesh Limited
CIIO	Critical Information Infrastructure Organization
CIRT	Computer Incident Response Team
CPTU	Central Procurement Technical Unit
CSE	Chittagong Stock Exchange
DGFI	Directorate General of Forces Intelligence
DoICT	Department of ICT
DSE	Dhaka Stock Exchange
ICT	Information on Communication Technology
ISPR	Inter-Services Public Relation
LEA	Law Enforcement Agency
NBR	National Board of Revenue
PGCB	Power Grid Company of Bangladesh
PMO	Prime Minister's Office
PPP	Public Private Partnership
RNPP	Rooppur Nuclear Power plant
SDN	Software Defined Network

This paper goes beyond merely identifying the challenges; it aims to contribute to the formulation of policy-oriented cybersecurity measures and provide recommendations for effective policy implementation. By synthesizing the available information, it aims to highlight the significance of a pragmatic and robust cybersecurity policy framework to safeguard Bangladesh's digital infrastructure as well as Critical Information Infrastructures of Bangladesh (CIIO's) and ensure the well-being of its citizens in cyberspace. The main contribution of the paper is–

- We comprehensively offer up-to-date analysis of different policies taken by the government.
- We also cover rising threats and the most common crimes in the cyberspace of Bangladesh
- Additionally, the authors represent a technical analysis and mention a customized method to prepare guidelines and justify the statistical analysis of this paper.

Organization: The rest of the paper is organized as follows. Section II presents a background study and literature review. Section III describes the statistics analysis and description. Section IV depicts the technical analysis of the study. Section V orients with issues and future discussion. Lastly, section VI summarizes with the conclusion.

II. BACKGROUND AND LITERATURE REVIEW

In recent times, the internet has become a necessity for connecting an individual to the whole world. This widespread transfer of valuable knowledge and information is cultivating numerous benefits and opportunities. However, the rapid growth in the number of Internet users brought along the challenging issue of cyber threats. The probability of cybersecurity being exploited is always on the rise due to the ever-evolving technological advancements in human life. The cybersecurity indexes involve several factors which include hackers, hardware manufacturers, software developers, and many more. Social media platforms are yet another area of exploitation for potential intruders who breach individual's data privacy. Facebook for instance has recently been the subject of such malware attacks (https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4). The reason behind such leaked portfolio of an individual can be traced to Facebook's access to 98 personal data points to promote advertisement to a person (https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that facebook-uses-to-target-ads-to-you/).

Cyber-attacks can be carried out from within the country or across the border. With this in mind, every other country needs to standardize its policies to prevent cyber threats. Bangladesh intends to continuously develop its socio-economic infrastructure. It is heavily reliant on its cyberspace infrastructure and is ever-increasing its dependency in this domain. This calls for Bangladesh to develop a reliable and efficient infrastructure capable of dealing with unwanted events. Cybersecurity concerns are now trending among public and private organizations. Previously, the country has been subjected to several cyber-attacks. The year 2012 resulted in 26 government organization attacks from offenders [11], [12]. The cybersecurity perspective in Bangladesh measured through indexes including the Global Cybersecurity Index (GCI), and the ICT Development Index signifies the requirement for significant upgradation in this area [13], [14]. A study revealed in a security report by Kaspersky showed Bangladesh ranked 2nd in the sphere of malicious infection (https://www.cirt.gov.bd/common-vulnerabilities-in-cyber space-of bangladesh/::text=AccordingFinancial institutes in Bangladesh also suffered from cyber-attacks in the past. The BGD e-Gov platform was invented after the notorious Bangladesh Bank reserve heist incident to prevent similar events from occurring. As per the Bangladesh e-Government Computer Incident Response Team, there has been a significant increase in registered events in the year 2018 (870 reported incidents) as compared to previous years https://www.cybersecurityintelligence.com/bgd-e– gov-cirt-3002.html. The significance of cybersecurity in Bangladesh has become evident following the cyber-attacks on critical financial infrastructures, such as the Bangladesh Bank, in 2016. These incidents highlighted the vulnerability of Bangladesh to cyber-attacks, which can be attributed to the inadequate availability of ICT resources and a shortage of skilled cybersecurity professionals to defend and protect the country's cyberspace [3].

As per Bangladesh's National Cybersecurity Strategy, the country's cyberspace is confronted with a wide array of attacks. These attacks encompass activities ranging from unauthorized surveillance aimed towards gaining critical information relating to politics to committing fraudulent activities concerning credit cards and relevant financial content. Furthermore, cyberattacks are now aimed at gaining access to the critical property of commercial enterprises operating in sectors such as communication, optics, and genetics [3] and [15].

In terms of the nature of cybercrime in Bangladesh, [4] refers to insights from an additional district judge. The judge highlights several categories of cybercrimes prevalent in the country, including:

- Sending malicious emails to foreign diplomatic missions and other VIPs.
- Distribution of pornography.
- Engaging in illegal activities through email.
- Spreading false and malicious information via the internet.
- Facilitating prostitution through online platforms.
- Using the Internet for women and child trafficking [4].

Several research works is dedicated to the current status of cybersecurity awareness in Bangladesh perspective. The authors in [16] presented a systematic analysis in regards to the awareness of cyber security amongst the common mass. The work also details recommendations and strategies that require implementation to raise awareness regarding the situation. The study presented in [13], [17] has analyzed the situation of cybersecurity in Bangladesh using internationally acclaimed indices. The research identifies the lack of proper framework from a legal perspective, while also highlighting the deficit in organizational ability and capacity building to develop the vision of Bangladesh to be digitally connected safely and reliably by 2030. In [18], the authors highlighted the awareness of cybercrime in Bangladesh. The work adopted Pearson's Chi-squared test to conduct an in-depth study of the situation and identified the urge to develop a prototype to tackle the issue. A detailed review is presented by researchers in [19] to emphasize the significance of cyber security to innovative and complex technologies concerning IoT, industrial automation, machine learning, e-commerce, and so on. The necessity for critical cyber defense and a data privacy policy, key vulnerability issues and their attacks on the cyberspace domain of Bangladesh, and strategies implemented to reduce these attacks are depicted by researchers in [20].

III. STATISTIC ANALYSIS AND DESCRIPCTION

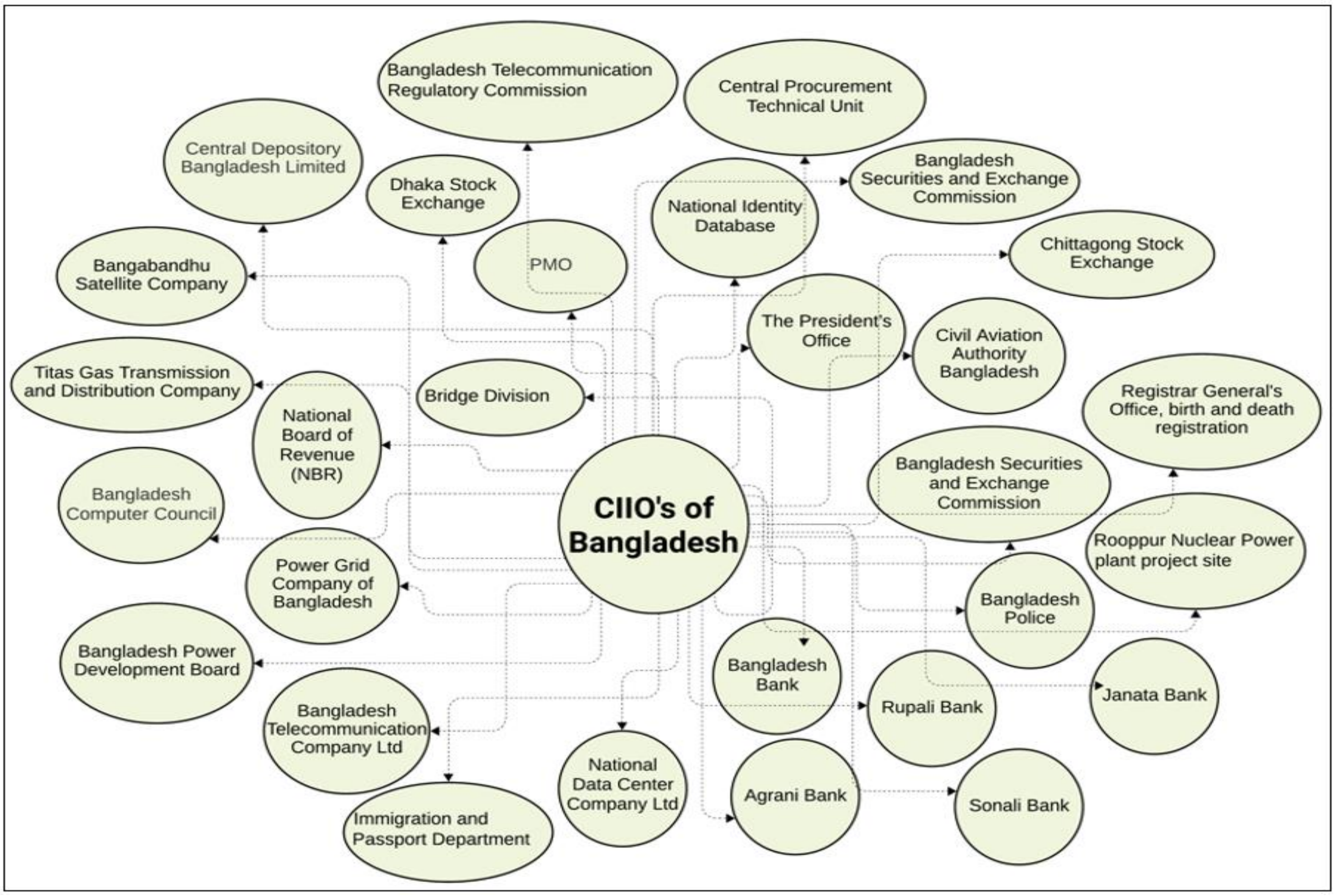
Bangladesh Telecommunication Regulatory Commission
Central Procurement Technical Unit
Central Depository Bangladesh Limited
Dhaka Stock Exchange
Bangladesh Securities and Exchange Commission
National Identity Database
PMO
Bangabandhu Satellite Company
Chittagong Stock Exchange
The President's Office
Civil Aviation Authority Bangladesh
Titas Gas Transmission and Distribution Company
National Board of Revenue (NBR)
Bridge Division
Registrar General's Office, birth and death registration
Bangladesh Computer Council
CIIO's of Bangladesh
Bangladesh Securities and Exchange Commission
Rooppur Nuclear Power plant project site
Power Grid Company of Bangladesh
Bangladesh Police
Bangladesh Power Development Board
Bangladesh Bank
Janata Bank
Rupali Bank
Bangladesh Telecommunication Company Ltd
National Data Center Company Ltd
Agrani Bank
Sonali Bank
Immigration and Passport Department

Fig 1 CIIO's of Bangladesh

Bangladesh's government declared 29 critical information infrastructures, and they are preparing security guidelines for their own. Fig. 1 represents different CIIOs of Bangladesh, and the ICT Divison under the Ministry of Posts, Telecommunications & Information Technology is taking care of this issue, collaborating with some organizations like the Bangladesh Computer Council (BCC) & Department of Information Communication and Technology (DoICT). BDG e-Gov CIRT is doing a brilliant job of securing Bangladesh's cyberspace. BDG e-GOV CIRT is currently the acting National CERT of Bangladesh.

Ongoing research and news reports provide insights into the nature of cybersecurity threats in Bangladesh. The following recent findings highlight key aspects of cyber threats in the country:

- Cyberbullying on the Rise: In 2022, the number of cyberbullying incidents has risen by 20 percent in contrast to the previous year. The Cyber Crime Investigation Division of Counter Terrorism and Transnational Crime received approximately 300 complaints related to cyberbullying in 2022, up from 220 in 2021. The majority (80 percent) of the victims were women, with 60 percent of female victims falling in the age group of 17 to 22 [21].
- Techniques Used by Cybercriminals: Cybercriminals employ various tactics to obtain personal information or gain unauthorized access to organizational computer systems. The state-run Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) has identified phishing, smashing, and fraudulent websites, malware, and insider threats as significant cyber threats. A report from BGD e-Gove CIRT reveals that spam is the most prevalent carrier of cyber threats in Bangladesh, as of 2021 [21].
- Limited Legal Assistance and Reporting: A study conducted by the Cybercrime Awareness Foundation indicates that more than 73 percent of cybercrime victims do not seek legal assistance. Among those who do seek assistance, over half of them find the support insufficient. Only 7 percent of victims receive the desired level of support. The study also reveals that 21 percent of respondents prefer to keep the matter confidential, 17 percent refrain from filing a complaint to protect their image, and 17 percent are afraid to report the incident due to potential harassment (Triune).
- Distributed Denial-of-Service (DDoS) Attacks: The Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT), a state-backed organization, has reported an increase in DDoS cyber-attacks in 2022. Approximately 240 major government organizations, commercial banks, ministries, and foreign ministries have experienced coordinated cyber-attacks. Notably, leading telecommunication companies such as “Grameenphone”, “RobiAxiata”, “Banglalink”, and “Teletalk” have also been targeted, causing disruptions in network communications and exposing vulnerabilities to malware infections [22].
- Banking Sector Cybersecurity: An analysis carried out by the Bangladesh Institute of Bank Management (BIBM) in 2022 examined the cybersecurity landscape of Bangladesh’s banking sector. The study concentrated on identifying the sources of cyber-attacks targeting banks in the country.

Cyber Risk in the Banking Sector: A study indicates that approximately 52% of banks in Bangladesh are classified as being at high cyber risk, with 32% at moderate risk and only 12% at low risk. The study emphasizes the significant cyber threat landscape faced by the banking sector, with an average of 630 cyberattacks targeting banks every day as represented in fig. 2 [23], [24].

Historical Cybersecurity Incidents in the Financial Sector: The financial sector in Bangladesh has experienced notable cyber-attacks in recent years. In 2015, a private bank faced an incident where bank accounts were hacked, resulting in unauthorized withdrawals. Furthermore, the network security of a government bank was compromised by attackers in 2015, gaining access to its website temporarily. Skimming attacks on six automated teller machine booths of three commercial banks. was another event that occurred in February 2016. One of the most significant incidents was the e-money laundering case in February 2016, where unauthorized access to Bangladesh Bank’s account resulted in the unwanted transfer of $101 million through the SWIFT system, although a portion of the stolen funds was recovered [25].

Types of Cyber Attacks in Bangladesh: According to [26], Cyber-Attacks on the Financial Sector in Bangladesh Have been Observed to Occur Through the Following Methods some are Explained below:

- Hacking of Bank Accounts: Incidents have been reported where cybercriminals gain unauthorized access to bank accounts, allowing them to carry out fraudulent activities such as unauthorized withdrawals.
- Network Security Disruption: Hackers have targeted the network security of financial institutions, leading to disruptions in their systems and services. This can result in temporary loss of website control and interruptions in normal banking operations.
- ATM Skimming: Skimming attacks on automated teller machines (ATMs) have been observed, where criminals install devices to gain access to customers’ banking card details and personal identification numbers (PINs) from unsuspecting customers.

Cyber Attacks in the Law Enforcement Agency (LEA) sector:Reasons for Cyber Attacks in Bangladesh: [25] identifies three key reasons for cyber-attacks across multiple sectors in Bangladesh:

- Financial Motives: Cybercriminals often target the financial sector due to the potential monetary gains associated with successful attacks. Financial institutions hold valuable assets and sensitive customer data [27], making them lucrative targets. Different types of attacks on financial sector are represented in fig. 3.
- Lack of Cybersecurity Measures: Insufficient implementation of robust cybersecurity measures within organizations can make them vulnerable to cyber-attacks. Weak security practices, outdated software, and inadequate employee awareness contribute to the increased risk.
- Growing Technological Dependency: With the rapid growth of technology adoption in various sectors, including finance, organizations become more dependent on digital systems and interconnected networks. This increased reliance on technology exposes them to a wider range of cyber threats. Fig. 4 represents different phishing campaigns that occur against the defense organization of Bangladesh.

➢ *Cyber Laundering and Reasons Behind it:*

- Money laundering is a significant cybercrime in Bangladesh, driven by various factors. [28] highlight the following reasons behind cyber laundering:
- Tax Evasion: Concealing financial information is often motivated by the evasion of taxes, where individuals or organizations attempt to avoid paying their due taxes.
- Lack of Political Transparency and Governance: Insufficient political transparency and ineffective governance can contribute to corruption across different sectors of society, providing an environment conducive to money laundering activities.
- Informal Economy: The prevalence of a large informal employment sector and high levels of informal transactions within the economy create numerous undefined sources, making it easier for illicit funds to be laundered.

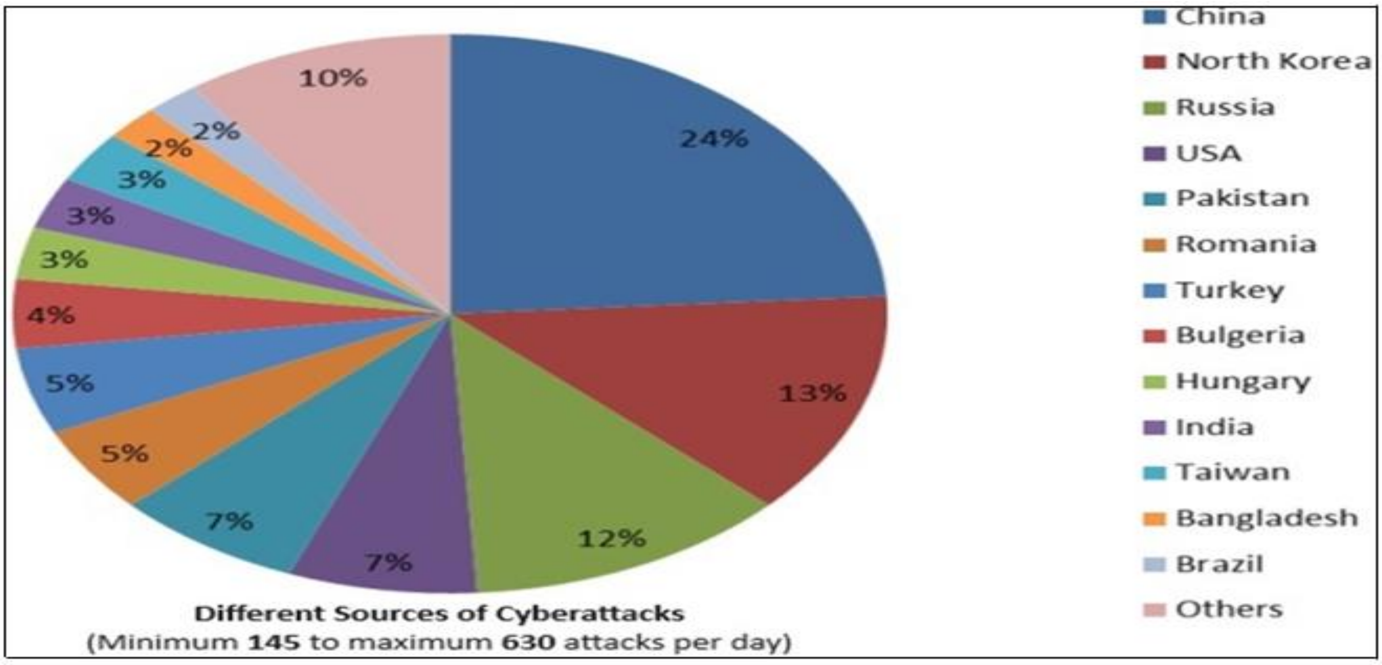

Fig 2 Sources of Cyber Attacks on the Banking Sector in Bangladesh
Source: the Business Standard, (2022)

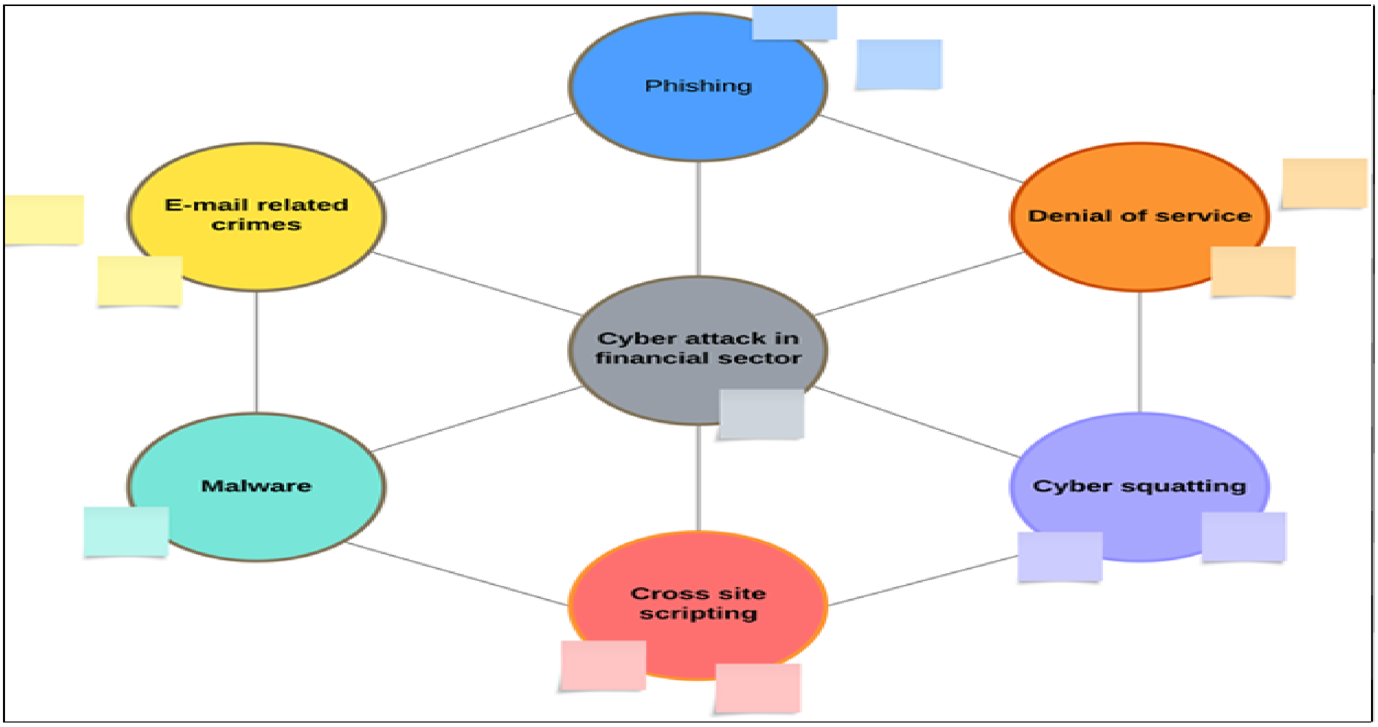

Fig 3 Cyber Attacks in Financial Sectors

Political Instability: Political instability can lead to capital flight, with individuals or entities seeking to transfer funds to external destinations as a means of safeguarding their assets. Digital Transformation and Data Localization in Bangladesh:

Since the launch of the government's" Digital Bangladesh" vision in 2008, Bangladesh has witnessed significant growth in internet subscribers and the development of its IT sector. Content creators, entrepreneurs, and various industries, including cooking channels on YouTube and education tech, have showcased the potential of digital platforms [7], [29]. Bangladesh's proposed Data Protection Act has generated discussion around data localization mandates. If passed into law, the bill would compel companies, government entities and NGOs operating in Bangladesh to store data within the country. Supporters contend localization reinforces data sovereignty and security. However, experts warn overly restrictive localization policies could hamper economic development and innovation. The draft law's Sections 44 and 45 outline localization rules that digital rights groups caution may enable increased surveillance and infringe on privacy. While localization does have merits, Bangladesh faces difficult trade-offs in balancing data control against participation in global digital ecosystems [8], [30]. As Bangladesh finalizes its data protection framework, nuanced policies will be needed to secure citizens' rights while still allowing beneficial cross-border data flows. The law's data provisions will significantly impact the country's cybersecurity, growth and technological advancement [31], [32].

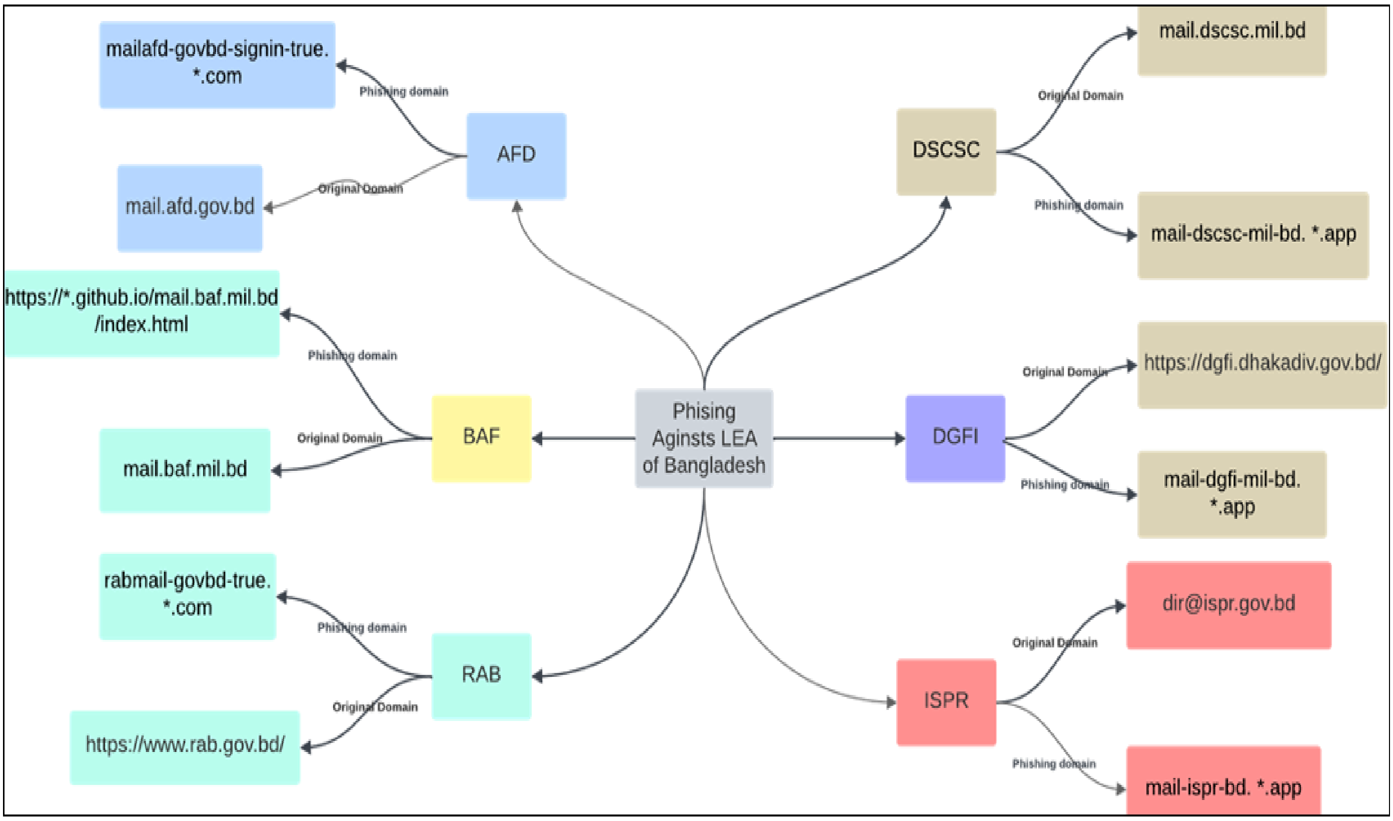

Fig 4 Phishing Campaign Against Military Organizations of Bangladesh

- *Cyber Security Challenges in Bangladesh*

Fig. 5 represents the basic reasons of every cyberattack occurs in Bangladesh. Bangladesh faces a range of challenges in ensuring cyber security and protecting the personal data, intellectual properties, and financial resources of its citizens. These challenges are prevalent across various sectors, including industry, government organizations, and academic and research institutions. The following are some of the key challenges:

Localization Policy and International Repercussions: Bangladesh's recent localization policy has raised concerns about its impact on the country's progress and international relationships. The localization of data can potentially anger international providers, leading to retaliatory actions by other countries [7].

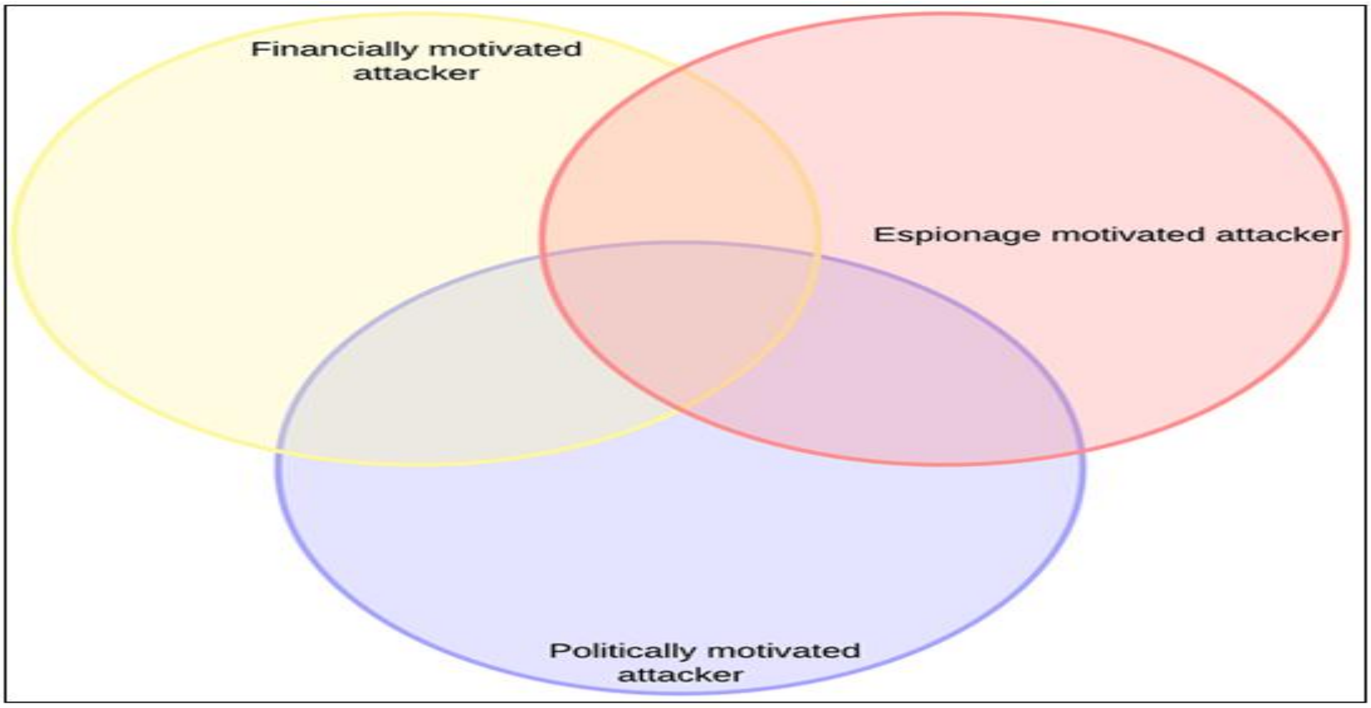
Financially motivated attacker
Espionage motivated attacker
Politically motivated attacker

Fig 5 Reasons of Cyberattacks in Bangladesh

- Cyber Laundering and Financial Sector Challenges: The financial sectors in Bangladesh, including banking, insurance, investment, and stock exchanges, face significant challenges due to cyber laundering. This practice involves the transfer of resources from the country to other nations, posing threats to financial stability [33].
- Pirated Software and Cybersecurity Vulnerabilities: The widespread use of pirated software in Bangladesh, estimated to be around 90%, exposes individuals and organizations to cybersecurity vulnerabilities. The use of unlicensed software increases the risk of malware infections and compromises overall security [34].
- Controversial Provisions of the Digital Security Act (DSA): Bangladesh's Digital Security Act of 2018, intended to provide cybersecurity to citizens, contains controversial clauses. The act's broad scope and vague provisions have been exploited for harassing individuals critical of the government, leading to a chilling effect on freedom of speech and expression (Triune) [35].
- Multiplicity of Cybercrimes: Bangladesh experiences a range of cybercrimes that directly harm individuals and society. These include hacking or cracking, illegal/unauthorized access, data interference, email spoofing, spamming, fraud, cyberstalking, defamation, drug trafficking, and more. Intellectual property crimes, vandalism of computer and network resources, theft of internet time and information, forgery, denial of services, and dissemination of obscene materials are also prevalent [34].

- Concerns Regarding Pornography and Child Exploitation: Bangladesh faces challenges related to pornography due to religious norms, values, and cultural restrictions. Child pornography is a particularly alarming issue, with criminals engaging in illegal activities such as hidden nude videos, manipulated images, and explicit footage. Victims' close relatives, including parents, family members, and relatives, are often targeted [34].
- Technological and Cultural Globalization: Technological advancements and cultural globalization in today's digitalized world can have both positive and negative impacts. While technology brings numerous benefits, it also introduces new vulnerabilities and risks. Adopting global technologies and cultural practices can sometimes conflict with the nation's norms, values, and cultural traditions, creating challenges in maintaining cyber security [34].

➢ *Prospects of Cyber Security in Bangladesh*

Bangladesh has made significant efforts to enhance cyber security and address the challenges posed by cyber threats to its national security. The country embraced its National Cyber Security Strategy in 2014, which outlines three key dimensions that need to be prioritized: legal steps, technical and procedural policies, and organizational structures [36]. The Ministry of Science and Information and Technology primarily regulates and controls cyber insecurities in Bangladesh and has implemented various strategies and frameworks to combat cyber threats and crimes. Examples of these include the National ICT Policy, Cyber Law, and Electronic Transaction Act [3]. To combat cybercrime effectively, Bangladesh has established a legal framework that includes several relevant acts and regulations. These legal measures encompass a range of aspects related to cyber security:

- Copyright Act, 2000 (Act No. 28 of 2000)
- The Code of Criminal Procedure, 1898
- Mutual Cooperation Act on Crime Related Matters, 2012 (Act No. 4 of 2012)
- Pornography Control Act, 2012 (Act No. 9 of 2012)

- Bangladesh Telecommunication Regulation Act, 2001 (Act No. 18 of 2001) [4]
- The country has adopted significant steps to combat illegal online transactions and cyber financial crimes:
- As an early member of the Asia Pacific Group on Money Laundering, Bangladesh has passed various laws and regulations, including the Money Laundering Prevention Act in 2002, updated in 2008 and 2009 [28].
- Additional measures include enacting the 2013 Money Laundering Prevention Rules.
- Bangladesh has established central and regional anti-money laundering task forces.
- An Anti-Money Laundering Department and Bangladesh Financial Intelligence Unit (BFIU) were created [28].
- The BFIU signed an agreement with the Anti-Corruption Commission to cooperate on investigating illicit finances [28].
- Through these legislative and institutional initiatives, Bangladesh aims to improve monitoring, reporting, and enforcement to tackle money laundering and cyber financial crimes.
- Ongoing partnerships between the government and the private sector will be key to effectively implementing the policies.
- By effectively implementing these legal frameworks and measures, Bangladesh can enhance cybersecurity and ensure the unauthorized or illegal use and access to data are addressed. The government and relevant institutions play vital roles and responsibilities in curbing cyber insecurities in the country. Policy Recommendations Several policy recommendations can be considered highly prospective in dealing with cyber-attacks and cyber insecurities in Bangladesh:
- Upgrade ICT Acts: The Information and Communication Technology (ICT) Acts should be upgraded to align with the United Nations Office on Drugs and Crime (UNODC) or the Convention on Cybercrime. This alignment will enable a clear definition and identification of cybercrime as outlined by UNODC.
- Amend the Digital Security Act: The Digital Security Act of 2018 should be amended to effectively identify cybercrime, ensure cybersecurity, and address any controversial provisions that violate human rights or serve political interests.
- Upgrade the Code of Criminal Procedure: The code of criminal procedure should be upgraded, if necessary, to ensure the proper investigation and trial of cybercriminals.
- Enhance International Cooperation: Increase international cooperation to ensure cybersecurity rather than relying solely on local cooperation. Cyber threats are transnational in nature, and collaborative efforts with other countries can strengthen cybersecurity measures.
- Consideration for Data Localization: Be cautious about data localization and its potential negative consequences. Localization of data and cyberspace can lead to political harassment and violations of human rights. Balancing data protection and privacy with cybersecurity is crucial.
- Promote Cybersecurity Awareness: Increase public awareness about safe internet use through proper training and education programs on cybersecurity and digital crimes. Empowering individuals with knowledge and skills can contribute to a safer online environment.
- Provide Access to Quality Technology: Ensure that good quality technology is accessible to the general population. This will enable individuals to protect themselves from becoming victims of malicious websites and crimes related to pornography.
- Invest in Research and Development: Allocate resources for research and development in the field of cybersecurity, specifically in developing new security systems for the financial sectors and information technology governance.
- Develop Responsiveness and Allocate Budget: Foster responsiveness among customers, bank managements, and personnel involved in state-sponsored cybersecurity initiatives. Adequate budget allocation is essential to support cybersecurity initiatives effectively.

IV. TECHNICAL ANALYSIS

Cybersecurity encompasses various techniques and strategies to protect computer systems, networks, and data from unauthorized access, attacks, and damage. Cybersecurity standards comprise technical guidelines and commonly accepted practices aimed at safeguarding the cyber environment and users within organizations that are connected to the internet. The cyber environment encompasses users, network infrastructure, hardware, software, processes, and services, whether located locally, in the cloud, or in transit. This includes information stored in system storage media that can be connected to the internet network, either directly or indirectly. The primary goal is to minimize risk by preventing or mitigating cyberattacks [37]. Numerous cybersecurity standards fall into distinct categories, with some existing as standalone standards like IEC 62351, IEEE 1686, ISO/IEC DIS 15408-1, ISO/IEC 27019, GB/T 22239. Others are categorized as standard series, exemplified by ISO/IEC 27000 and IEC 62443 (ISA 99), while certain standards are framed as regulations, as seen in the case of NERC CIP [38].

Although there are many techniques in this paper, OSINT (Open-Source Intelligence) is implemented to analyze the data. Fig. 6 describes the process of OSINT which is implemented in this study. OSINT is a method of gathering in-formation from publicly available sources. After observations done and the semantic processing completed the decision is made applying the OSINT approach. The process typically involves several steps [39], [40]:

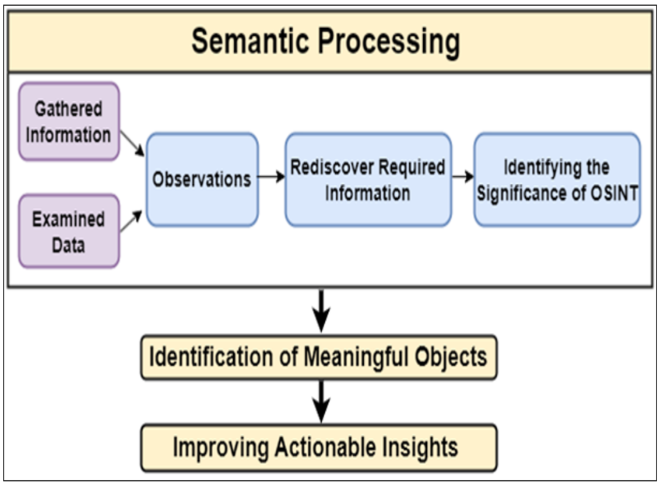
Semantic Processing
Gathered Information
Examined Data
Observations
Rediscover Required Information
Identifying the Significance of OSINT
Identification of Meaningful Objects
Improving Actionable Insights

Fig 6 Process of Technical Analysis

- Define Objectives: Determine what information you need and why you need it. This helps focus your search.
- Collection: Gather data from open sources such as the internet, social media, public records, news articles, academic papers, and more. Tools like search engines, social media monitoring platforms, and databases are commonly used.
- Verification: Assess the credibility and reliability of the gathered information. Cross-reference multiple sources to confirm accuracy.
- Analysis: Organize and analyze the collected data to extract meaningful insights. This involves identifying patterns, connections, and relationships between different pieces of information.
- Reporting: Present findings in a clear and understandable format, tailored to the audience. Reports might include summaries, visualizations, or recommendations based on the analyzed data.
- Iterate: Revisit objectives, gather more data, or refine analysis as needed. OSINT is an ongoing process that may require continuous adjustments based on new information or changes in objectives.

Throughout the OSINT process, it’s essential to respect legal and ethical boundaries, ensuring that the information is obtained and used responsibly and within legal frameworks [41]. When gathering and examining open data sourced from the Internet, challenges arise due to the processing of extensive volumes, the necessity to search and navigate dynamic information flows, and the abundance of multilingual dynamic information resources leading to information noise. This complexity hinders the efficient discovery of required information and timely operational analysis, underscoring the significance of employing OSINT in information and analytical tasks.

The predominant issues, particularly in the semantic processing of vast dynamic text datasets, are relevant today. Various technological concepts such as Big Data, Complex Net-works, Cloud Computing, and Data/Text Mining are presently utilized to address these challenges.

Globally, effective analytical processing of information from global networks, swift extraction of essential factual data, identification of trends in specific subject areas, recognition of meaningful anomalies, and forecasting remain unresolved tasks. Many of these challenges are inherent problems in the semantic processing of extensive dynamic data arrays. Even partial attempts to practically address these issues significantly impact the success of projects like Google, Yandex, Baidu, KeyholeOSINT (integrated into cyber defense systems such as social network monitoring systems like SMM), Brandwatch, CyberAlert, YouControl, as well as analytical systems like Palantir, Centrifuge, among others.

An ontological approach is increasingly adopted for constructing subject domain models, particularly in the realm of cybersecurity. Within the OSINT framework, various theoretically justified tools have been developed for building domain models, including distributed content monitoring of global networks, the creation of multilingual full-text databases, analysis of thematic information flow dynamics, identification of terminological bases in subject areas, formation of networks depicting interrelations of concepts extracted from text arrays, and identification of implicit connections among objects.

V. ISSUES AND FUTURE DISCUSSION

A. Open Issues

Some common issues people are facing like where to ask for help, to whom application to be submitted, which organization will take care of the fact etc. are still a challenge for the rural people of South Asian countries like Bangladesh. In this paper, we have mentioned 29 CIIO’s of Bangladesh of which the ICT Division is one and leading from the front. ICT Division along with the cooperation of LEA (Law Enforcement Agency) will advise and in some cases will take necessary steps to solve the issues. In this case, a GD (General Dairy) from a police station is necessary [42].

Some more issues like cyberbullying, spam, identity theft, ransomware, web-based attacks, and the lists are rising day by day in Bangladesh. Although the Government of Bangladesh has already taken some important steps these issues remain unsolved because people are still showing negligence in com-plying with these mentioned guidelines and protocols. Once people become careful of their cyber footprint, the number of unsolved issues will be decreased [43].

B. Future Discussion

Based on the discussion throughout the research, in this part, we present some potential future aspects as follows.

Computer Vision: Computer vision and sign recognition which will work alongside AI-Powered Defense. Expect to see more sophisticated AI-driven cybersecurity tools. These AI models will not only detect but also autonomously respond to threats in real-time, improving overall defense mechanisms [44].

Data Storing: Data storing capacity will be increased using a custom QR code generation method for reference [45], [46].

Quantum Computing Impact: Quantum computing's advent poses both a threat and a solution. While it can potentially break existing encryption, it might also offer robust cryptographic solutions that are quantum-resistant. [47] offers a model for performance benchmarking.

Impact of Security Architecture for Industry 4.0: Different security architecture along with standardization will bring new framework for securing cyber ecosystem of Bangladesh.

With the passage of time, we might move to the fusion energy sector. A proper guideline is a must while securing a fusion power plant [48]. While detecting cyber criminals with minimum available data, we can go with [49], which will help detect cyber criminals with minimum segmented data captured through web intelligence and social media. IoT devices are very vulnerable in terms of cybersecurity. Many recent cases show that in the field of healthcare wearable IOT devices, privacy, and security must be ensured [50].

VI. CONCLUSION

As technology and information science advance, the use of computers, the internet, and ICT has become integral to various sectors. While technology has brought positive changes, it has also introduced cybersecurity risks and insecurities. In Bangladesh, the use of technology is rapidly increasing across industries and organizations, resulting in higher cybersecurity risks. Although legal and institutional frameworks for cyber-security exist in Bangladesh, they do not meet international standards and lack practical effectiveness. Moreover, there is a shortage of skilled cybersecurity professionals and technical equipment needed for effective cyberspace protection. Considering these challenges, the government and relevant ministries should proactively implement pragmatic policies and plans. Adequate resources, funding, and logistical support must be made available to ensure cybersecurity and the well-being of Bangladesh's individuals, organizations, industries, and academia. By undertaking these initiatives and prioritizing stress-free data and internet usage, the field of cybersecurity can become more secure and sustainable in the future.

REFERENCES

[1]. N. Kshetri, "Cybercrime and cybersecurity in africa," pp. 77–81, 2019.

[2]. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescape, M. Hasan, M. Sookhak, and A. Mosavi, "Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot," IEEE Access, vol. 9, pp. 28 361–28 376, 2021.

[3]. M. T. Islam, M. F. Islam, and J. Sawda, "E-commerce and cyber vulnerabilities in bangladesh: A policy paper," International Journal of Law and Society (IJLS), vol. 1, no. 3, pp. 184–202, 2022.

[4]. M. Murshed, "A comparative analysis between bangladeshi and korean legal frameworks for combating cybercrime to ensure cyber security," Kor. UL Rev., vol. 19, p. 23, 2016.

[5]. M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, "Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3850–3864, 2022.

[6]. Rahman, T. Debnath, D. Kundu, M. S. I. Khan, A. A. Aishi, S.Sazzad, M. Sayduzzaman, and S. S. Band, "Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities," AIMS Public Health, vol. 11, no. 1, pp. 58–109, 2024.

[7]. S. S. Diwan, "Next episode: the story of video streaming viewership in india," Ph.D. dissertation, University of British Columbia, 2023.

[8]. Rahman, M. J. Islam, M. R. Karim, D. Kundu, and S. Kabir, "An intelligent vaccine distribution process in covid-19 pandemic through blockchain-sdn framework from bangladesh perspective," in 2021 Inter-national Conference on Electronics, Communications and Information Technology (ICECIT), 2021, pp. 1–4.

[9]. Rahman, C. Chakraborty, A. Anwar, M. Karim, M. Islam, D. Kundu, Rahman, S. S. Band et al., "Sdn–iot empowered intelligent frame-work for industry 4.0 applications during covid-19 pandemic," Cluster Computing, vol. 25, no. 4, pp. 2351–2368, 2022.

[10]. Rahman, U. Sara, D. Kundu, S. Islam, M. J. Islam, M. Hasan, Z. Rahman, and M. K. Nasir, "Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture," International Journal of Advanced Computer Science and Applications, vol. 11, no. 9, 2020.

[11]. K. Sarker, H. Rahman, K. F. Rahman, M. S. Arman, S. Biswas, and Bhuiyan, "A comparative analysis of the cyber security strategy of bangladesh," arXiv preprint arXiv:1905.00299, 2019.

[12]. T. A.-U.-H. Bhuiyan, S. Ahmed, M. Salahin, M. Pollab, J. N. Jui, M. T. Ahmmed, A. Rahman, and M. A. H. Wadud, "Iot-based patient monitor-ing system through online cloud and ecg sensor," in 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM). IEEE, 2023, pp. 1–6.

[13]. T. H. Chowdhury, N. Parvez, S. S. Urmi, and K. A. Taher, "Cybersecurity challenges and policy options for bangladesh," in 2021 International Conference on Information and Communication Technology for Sustain-able Development (ICICT4SD). IEEE, 2021, pp. 472–476.

[14]. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, "Distblocksdn: A distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities," in 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019, pp. 1–6.

[15]. F. Cristiano, “Israel: Cyber-securitization as national trademark,” Rout-ledge Handbook of Global Cybersecurity Strategy. Abingdon: Routledge, 2020.

[16]. Al Mamun, J. B. Ibrahim, and S. M. Mostofa, “Cyber security awareness in bangladesh: An overview of challenges and strategies,” Int. J. Comp. Sci. Informat. Technol. Res, vol. 9, pp. 88–94, 2021.

[17]. M. S. Ahammad and A. Rahman, “A framework for m-health services using 4g (lte) technology,” International Journal of Innovative Science and Research Technology, vol. 5, pp. 1085–1095, 2020.

[18]. N. Ahmed, U. Kulsum, I. B. Azad, A. Z. Momtaz, M. E. Haque, and M. S. Rahman, “Cybersecurity awareness survey: An analysis from bangladesh perspective,” in 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC). IEEE, 2017, pp. 788–791.

[19]. M. Rahaman, “Recent advancement of cyber security: Challenges and future trends in bangladesh,” Saudi Journal of Engineering and Tech-nology, vol. 7, no. 6, pp. 278–289, 2022.

[20]. Haque, “Need for critical cyber defence, security strategy and privacy policy in bangladesh-hype or reality?” arXiv preprint arXiv:1906.01285, 2019.

[21]. N. M. Zawad, “Cyber security in bangladesh: An overview of threats and prospects.”

[22]. M. J. Hossain, R. H. Rifat, M. H. Mugdho, M. Jahan, A. A. Rasel, and M. A. Rahman, “Cyber threats and scams in fintech organizations: A brief overview of financial fraud cases, future challenges, and rec-ommended solutions in bangladesh,” in 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE, 2022, pp. 190–195.

[23]. N. Capuano, G. Fenza, V. Loia, and C. Stanzione, “Explainable artificial intelligence in cybersecurity: A survey,” IEEE Access, vol. 10, pp. 93 575–93 600, 2022.

[24]. Rahman, M. S. Hossain, G. Muhammad, D. Kundu, T. Debnath, Rahman, M. S. I. Khan, P. Tiwari, and S. S. Band, “Federated learning-based ai approaches in smart healthcare: concepts, taxonomies, challenges and open issues,” Cluster computing, vol. 26, no. 4, pp. 2271– 2311, 2023.

[25]. N. A. Siddique, “Framework for the mobilization of cyber security and risk mitigation of financial organizations in bangladesh: a case study,” 2019.

[26]. Z. Zahoor, M. Ud-din, and K. Sunami, “Challenges in privacy and security in banking sector and related countermeasures,” International Journal of Computer Applications, vol. 144, no. 3, pp. 24–35, 2016.

[27]. S. Islam, U. Sara, A. Kawsar, A. Rahman, D. Kundu, D. D. Dipta, A. R. Karim, and M. Hasan, “Sgbba: An efficient method for prediction system in machine learning using imbalance dataset,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 3, 2021.

[28]. N. Joveda, M. T. Khan, A. Pathak, and B. Chattogram, “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, vol. 11, no. 10, pp. 54–65, 2019.

[29]. Rahman, K. Hasan, D. Kundu, M. J. Islam, T. Debnath, S. S. Band, and N. Kumar, “On the icn-iot with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives,” Future Generation Computer Systems, vol. 138, pp. 61–88, 2023.

[30]. M. Faisal, H. Siddiqua, M. J. Islam, and A. Rahman, “An sdn-based se-cure model for iot network in smart building,” in 2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI), 2022, 1–6.

[31]. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, “Towards a blockchain-sdn-based secure architecture for cloud computing in smart industrial iot,” Digital Communications and Networks, vol. 9, no. 2, pp. 411–421, 2023.

[32]. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, M. Sookhak, P. Tiwari, and N. Kumar, “Impacts of blockchain in software-defined internet of things ecosystem with network function virtualization for smart applications: Present perspectives and future directions,” International Journal of Communication Systems, p. e5429, 2023.

[33]. M. A. Islam, A. Nabi, M. Rahman, M. Islam, D. Ahmed, A. S. G. Faruque, A. Hossain, A. van Belkum, and H. P. Endtz, “Prevalence of faecal carriage of ndm-1-producing bacteria among patients with diarrhoea in bangladesh,” Journal of medical microbiology, no. 4, pp. 620–622, 2014.

[34]. M. N. Nabi and M. T. Islam, “Cyber security in the globalized world: Challenges for bangladesh,” Economic and Social Development: Book of Proceedings, p. 32, 2014.

[35]. M. T. Ahmed, R. Islam, M. A. Rahman, M. J. Islam, A. Rahman, and S. Kabir, “An image-based digital forensic investigation framework for crime analysis,” in 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM). IEEE, 2023, pp. 1–6.

[36]. W. Dukes, “Committee on national security systems (cnss) glossary, cnssi no. 4009,” DoD Ft Meade, 2015.

[37]. M. Syafrizal, S. R. Selamat, and N. A. Zakaria, “Analysis of cyberse-curity standard and framework components,” International Journal of Communication Networks and Information Security, vol. 12, no. 3, pp. 417–432, 2020.

[38]. R. Leszczyna, “Standards on cyber security assessment of smart grid,” International Journal of Critical Infrastructure Protection, vol. 22, pp. 70–89, 2018.

[39]. V. Lande and E. V. Shnurko-Tabakova, “Osint as a part of cyber defense system,” 2019.

[40]. S. I. Khan, A. Shahrior, R. Karim, M. Hasan, and A. Rahman, "Multinet: A deep neural network approach for detecting breast cancer through multi-scale feature fusion," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 8, pp. 6217–6228, 2022.

[41]. Yeboah-Ofori and A. Brimicombe, "Cyber intelligence and osint: Developing mitigation techniques against cybercrime threats on social media," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 7, no. 1, pp. 87–98, 2018.

[42]. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. P. Mahmud, M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," IEEE Access, vol. 8, pp. 209 594–209 609, 2020.

[43]. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom, and M. Razaul Karim, "Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network," in 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1–6.

[44]. M. A. Rahaman, K. U. Oyshe, P. K. Chowdhury, T. Debnath, A. Rahman, and M. S. I. Khan, "Computer vision-based six layered convneural network to recognize sign language for both numeral and alphabet signs," Biomimetic Intelligence and Robotics, p. 100141, 2023.

[45]. I. Udoy, M. A. Rahaman, M. J. Islam, A. Rahman, Z. Ali, and G. Muhammad, "4sqr-code: A 4-state qr code generation model for increasing data storing capacity in the digital twin framework," Journal of Advanced Research, 2023.

[46]. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, and B. Minaei-Bidgoli, "Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management," IEEE Access, vol. 8, 140 008–140 018, 2020.

[47]. T. Lubinski, S. Johri, P. Varosy, J. Coleman, L. Zhao, J. Necaise, C. H. Baldwin, K. Mayer, and T. Proctor, "Application-oriented performance benchmarks for quantum computing," IEEE Transactions on Quantum Engineering, 2023.

[48]. Joseph, Y. Shi, M. Porter, A. Castelli, V. Geyko, F. Graziani, Libby, and J. DuBois, "Quantum computing for fusion energy science applications," Physics of Plasmas, vol. 30, no. 1, 2023.

[49]. T. Debnath, M. M. Reza, A. Rahman, A. Beheshti, S. S. Band, and Alinejad-Rokny, "Four-layer ConvNet to facial emotion recognition with minimal epochs and the significance of data diversity," Scientific Reports, vol. 12, no. 1, p. 6991, dec 2022. [Online]. Available: https://www.nature.com/articles/s41598-022-11173-0

[50]. Rahman, M. Rahman, D. Kundu, M. R. Karim, S. S. Band, and Sookhak, "Study on iot for sars-cov-2 with healthcare:present and future perspective," Mathematical Biosciences and Engineering, vol. 18, no. 6, pp. 9697–9726, 2022