International Journal of Humanities Arts and Business (IJHAB)
ISSN: 2709-0604 (Print)
ISSN: 3006-4805 (Online)
Volume-02, Issue-02, pp-9-17
www.ijhab.com

Research Paper Open Access

Significance of Cyber Security for Smart Bangladesh: A Brief Review

Md Nadimul Haque Noman[1]

[1]*Sub-Inspector, Badda Police Station, Gulshan Division, Dhaka Metropolitan Police (DMP), Bangladesh Police*

Corresponding author: Md Nadimul Haque Noman, Sub-Inspector, Badda Police Station, Gulshan Division, Dhaka Metropolitan Police (DMP), Bangladesh Police, email: nhn.english.ju@gmail.com

Citation: Noman, M. N. H. (2024). Significance of Cyber Security for Smart Bangladesh: A Brief Review. *International Journal of Humanities Arts and Business (IJHAB)*; Vol-2, Issues-2.

ABSTRACT : *Today, various countries around the world have embraced new technology in order to become smart countries. New technologies improve the lives of citizens. The adoption of any technology, however, provides additional concerns and challenges. A vulnerable move by an individual or group in a smart country can put the entire country at danger. Since numerous components of a smart nation rely on information and communication technology, cyber-security issues (such as information leakage and harmful cyber-attacks) in this field influence smart country behavior. As a result, in order to respond to the enthusiastic acceptance of global smart technologies, cyber security must evolve in the same direction. The goal of this study is to review relevant literatures on cyber security, smart country, and the available relevant literature smart technology. The current study further focuses on the basic components of a smart country, as well as the Bangladesh government's initiatives to make the country smart. The article also discusses potential cyber security concerns and significance of them. According to the study, developing adaptable systems with excellent information protection capabilities is critical to preventing significant security catastrophes, which can result in disastrous financial, data, credit, and public trust losses.*

Keywords- : Bangladesh, smart country, digital technology, cyber security

I. INTRODUCTION

A "smart country" is one that uses innovation, technology, and data to advance its infrastructure, economy, governance, and people's quality of life (Witanto, Lim, & Atiquzzaman, 2018). It is a development of the idea of a "smart city" in which the concepts are used on a national level. A smart country enhances productivity, sustainability, and service quality across sectors by utilizing digital technology, connectivity, and data-driven decision-making (Lim, Cho, G.-H., Kim, 2021). Strong digital infrastructure, including widespread high-speed internet access, online platforms for public services, and data collection techniques, are characteristics of a smart country (Ijaz, et al., 2016). Additionally, residents would be able to access government services online, paying taxes, applying for permits, and more without physically visiting government offices (Khatoun, Zeadally, 2017). It is critical to keep in mind that creating a highly smart country involves a lot of challenges, including infrastructure investment, data privacy issues, cyber security risks, and ensuring equitable access to technology for all citizens (Lee, Kim, & Seo, 2019). Furthermore, based on each nation's resources, goals, and technological advancements, the degree of "smartness" differs tremendously (Witanto, Lim, & Atiquzzaman, 2018). To keep pace with the world, the government of Bangladesh want to turn this

country into a smart one. An effort called ‘Smart Bangladesh’, spearheaded by the Bangladeshi government, aims to make Bangladesh a sustainable society with cutting-edge technology is the core issue of the present study.

II BACKGROUND OF SMART BANGLADESH

At the Digital Bangladesh Day-2022 event held at the Bangabandhu International Conference Center (BICC) in the capital on December 12, 2022, Prime Minister Sheikh Hasina made the first mention of creating a "Smart Bangladesh" during her remarks as the Chief Guest (Jibon, 2023**)**. "We will turn Bangladesh into a developed country in the year 2041, and Bangladesh will go from Digital Bangladesh to Smart Bangladesh," Sheikh Hasina declared (Prothom Alo. 2023). On the website of Aspire to Innovate (a2i), run by the Bangladesh government, we observe four indicators of Smart Bangladesh (Jibon, 2023). The four fundamental pillars of Smart Bangladesh are 1) Smart Citizens, 2) Smart Government, 3) Smart Society, and 4) Smart Economy. In this context, ‘smart’ refers to the application of advanced technologies such as Artificial Intelligence (AI), Internet of Things (IoT), Machine Learning (ML), deep learning (DL), Block-chain, Big Data, Robotics, Drone technology, 3D printing, Nanotechnology, Quantum computing, and other cutting-edge technologies to improve various national aspects.

2.1 Plan for the Smart Bangladesh

'Smart Bangladesh' is built on four pillars. Smart governance, smart citizens, and smart society. There will be no more transition to Smart Bangladesh if we move forward by recognizing these four particular areas in the development of Smart Bangladesh (Prothom Alo, 2023**)**. Smart individuals and a smart government will transform all services and media to digital (Maruf, et al., 2020). Additionally, if a smart economy and smart society can guarantee growth, they will contribute to the development of an inclusive society and a business-friendly environment (BASIS, 2022).

'Smart Bangladesh will be cost-effective, sustainable, knowledge-based, intelligent and innovative (Jibon, 2023). In short, everything will be smart. Such as ensuring smart healthcare, smart transport, smart utilities, urban administration, public safety, agriculture, internet connectivity and disaster management for implementation of smart cities and smart villages (BASIS, 2022). One student, one laptop, one dream initiative has been proposed to ensure online participation of students. Under this, all digital services will be brought under a centrally integrated cloud. The Bangladesh government has already changed the name of the Digital Bangladesh Task Force to 'Smart Bangladesh Task Force' (BASIS, 2022).

2.3 Components of Smart Bangladesh

With the four main pillars of the Smart Bangladesh Plan—Smart Citizen, Smart Government, Smart Economy, and Smart Society—that were previously stated by the Honorable Prime Minister.

Smart Citizen

"Smart Citizen" typically refers to the concept of using technology, data, and citizen engagement to create more efficient, sustainable, and livable cities (Qamar, & Bawany, 2020). It involves the integration of various technological solutions and data-driven approaches to enhance urban infrastructure, services, and overall quality of life for residents (Secinaro, et al., 2021). Smart Citizen initiatives often involve deploying sensors and IoT (Internet of Things) devices throughout the city to gather data on various parameters such as air quality, noise levels, traffic patterns, waste management, energy consumption, and more (Sengan, et. Al., 2020). This data is then analyzed to gain insights into urban challenges and trends. he involvement of citizens in data collection and decision-making is a fundamental aspect of the Smart Citizen concept (Vitunskaite, 2019). Citizens can participate by contributing data, sharing feedback, and collaborating with city officials to address issues and prioritize projects (Secinaro, et al., 2021).

Smart Government

Utilizing ICT integration for planning, management, and operations at any level or across layers, smart government creates value for sustainable public production (Chen, Wawrzynski, 2021). To put it another way, in a smart government, information and communication technology-based business processes are what enable the flow of continuous information between the government and the delivery of high-quality services (Sengan, et. Al., 2020). The next phase of e-government is smart governance (Chatfield and Reddick, 2019). Instantaneous information is used by the smart government to prevent crime by raising the level of situational awareness, responding to accidents quickly and effectively, looking into emergencies, and enhancing municipal services (Witanto et al., 2018).

Smart Economy

A "smart economy" refers to an economic system that leverages technological advancements and data-driven strategies to enhance productivity, innovation, and overall efficiency (Chen, 2021). It involves the integration of various technologies such as the Internet of Things (IoT), artificial intelligence (AI), block chain, data analytics, and more to transform traditional industries and business processes (Chatfield, and Reddick, 2019). The concept of a smart economy is closely related to the broader idea of a "smart city," where similar principles are applied to urban development, infrastructure, and services to create efficient, sustainable, and livable environments for residents (Barr, et al., 2021). It's important to note that the realization of a smart economy requires collaboration among governments, businesses, academia, and the general population to create an ecosystem that can fully harness the potential of technology and innovation for economic growth and societal benefit (Chen, 2021).

Smart Society

A "smart society" refers to a concept where advanced technologies and data-driven approaches are integrated into various aspects of daily life to improve efficiency, sustainability, and quality of life for its citizens (Baig, et al., 2017). It encompasses the integration of Internet of Things (IoT) devices, artificial intelligence (AI), data analytics, and other emerging technologies to create interconnected and intelligent systems that enhance various domains, such as urban planning, healthcare, transportation, energy management, and more (Atitallah, et al., 2020). However, it's important to consider potential challenges and concerns associated with a smart society, including data privacy, cyber security, digital divide (inequality in access to technology), and the ethical implications of AI and automation (Al-Saidi, Zaidan, 2020). Balancing technological advancements with societal well-being and inclusivity is crucial for realizing the full potential of a smart society (Al-Dakheel, et al., 2020).

Cyber Security

Cyber security refers to the practice of protecting computer systems, networks, programs, and data from digital attacks, unauthorized access, and other forms of cyber threats (Al-Ghamdi, 2021). With the increasing reliance on technology and the internet, cyber security has become a critical concern for individuals, businesses, governments, and organizations worldwide (Ahmed et al., 2021). It encompasses various measures and strategies aimed at safeguarding digital assets and ensuring the confidentiality, integrity, and availability of information (Baig, et al., 2017). This involves securing computer networks and their components, such as routers, firewalls, and intrusion detection systems, to prevent unauthorized access and data breaches (Chen, Wawrzynski, 2021). Protecting sensitive data from unauthorized access, modification, or disclosure. Encryption, access controls, and data classification are commonly used techniques (Qamar, & Bawany, 2020). The field of cyber security is vast and complex, requiring expertise in technology, law, psychology, and other disciplines to effectively address the diverse range of threats (Ahmed et al., 2021).

III OBJECTIVES OF THE STUDY

The main objective of this study is to explore the significance of cyber security in materializing the plan of smart Bangladesh.

IV METHODOLOGY

The paper is prepared based on secondary data, which collected from different sources like books, journals, sewspaper and the internet. Collected information has been analyzed to draw suggestion from the study and make the study informative to the concerned readers. The researcher selected the literatures based on their acceptably, reliability and relatability. Besides, the main inclusion criteria for the literatures for review was whether they were related the goals and objectives or not. The researcher did not consider literatures from unauthentic and unrecognized sources and the literatures that were not related to the aims of the current study. Data from selected studies were extracted and summarized using a standardized approach. This involved categorizing key concepts, patterns themes, and gaps in the literatures. The researcher also consulted with stakeholders and experts in the related field to ensure that all relevant literature was captured and to validate the findings.

V FINDINGS

The National Cyber security Strategy, NCS, (2018) outlined a total of 11 actions, including raising public awareness, reducing cybercrime, establishing incident response capabilities, protecting critical infrastructure, developing a national cyber security framework, securing government infrastructure, developing cyber security skills and training, and establishing public-private partnerships. These activities were all related to national threats, priorities, and goals, as well as to business growth. The strategy listed various national risks and threats, such as espionage aimed at gathering political intelligence, intellectual property theft from businesses, unauthorized modification, distributed denial of service attacks and disruption during the patching of smart meters, phishing to facilitate credit card fraud, and malware attacks (CCRB, 2018**)**. Responsibility for the design, implementation, monitoring and revision of the strategy has not been formally assigned to any authority, but the process has been and continues to be led by the Ministry of Posts, Telecommunications and Information Technology (MPTIT).

5.1 Security for Smart Citizens

Cyber security for smart citizens refers to the practices and measures the government and individuals can take to protect them and their personal information in an increasingly connected and digital world. As more devices, services, and processes become "smart" and connected to the internet, the potential for cyber threats and attacks also increases. A smart citizen is primarily connected to the social infrastructure of a smart city. Smart cities depend heavily on smart citizens for innovation, productivity, and smart living. As a result, a smart nation's role is crucial in helping its citizens grow into smart individuals. Higher education institutions can be enlisted by the government to serve as knowledge intermediaries, managers, and suppliers of educational resources to help the populace become more knowledgeable. Two key technologies utilized to create smart applications that improve teaching, learning, and knowledge sharing are artificial intelligence (AI) and big data. Additionally, it is important to involve individuals in the e-government system through the usage of IoT, as this will enable informed citizens to engage with public services as proactive stakeholders and improvers. Nonetheless, there may be issues with people accepting the security and privacy of the data and services that are offered to them. Additionally, social consciousness and health care are two more essential components of intelligent citizens. Healthcare can be provided by using ICT to offer emergency help and real-time monitoring of particular care needs. It is also important to note that smart economies employ ICT to support smart inhabitants with automated lighting, heating, and security systems that are networked and internet enabled. Smart citizens can live smarter lives thanks to these technological advancements. Applications for smart citizen assistance are frequently utilized in smart homes. Since these applications collect users' personal and private information, privacy and security concerns must be transparently addressed. Empowering technologies like cloud computing and storage, artificial intelligence (AI), machine learning, data mining, and wireless sensor networks enable smart living applications.

Therefore, it is essential to establish guidelines and standards for smart application development in order to identify and control the risks connected to them. The government must develop proper security

protocol for protecting citizens' data and devices and at the same time a strong monitoring system should be developed by the government. The government also should impart technology education and technology awareness to the citizens so that they can Stay informed about the latest cyber threats and security best practices and know about common hacking techniques like social engineering and phishing. By following these practices, the government can significantly reduce the risk cyber-attacks on citizens and enhance their overall cyber security as a smart citizen. It's important to remember that cyber security is an ongoing process, and staying vigilant is key to staying safe in the digital age.

5.2 Security for Smart Economy

A smart economy is one that is innovative, competitive, and makes responsible use of resources while utilizing information and communication technology across all sectors. Within the framework of the smart economy, we regularly use internet-based platforms like Uber, Airbnb, Alibaba, Amazon, and so on. These platforms monopolize the market because they consolidate and control the gathering and processing of information. Platforms are useful for specific services and goods, but in order to make a purchase through them, personal data and information must be provided. For the smart economy, it poses a risk. Additionally, another innovation of the smart economy is the sharing economy, which provides coordinated access to products and services through internet platforms. People participate in the smart economy through the share of services like accommodation, car, bike, and so forth. Furthermore, for quick and easy financial transactions, people in smart countries likely use a variety of smartphone apps, e-cards, e-transaction systems, ATMs, etc. As a result, though the digital economy promotes digital industries and innovations as well as public participation and engagement in all spheres of life, users' privacy about their data might be at risk. So, cyber security is a critical aspect of building and maintaining a smart economy. To ensure the security and resilience of a smart economy, several cyber security measures need to be considered.

The government must protect the communication channels that connect devices, sensors, and systems. They should implement strong encryption protocols, firewalls, intrusion detection and prevention systems, and regularly update and patch network infrastructure. Implementation of encryption for data at rest and in transit should be ensured. Any type of data access should be limited only to authorized personnel or devices. Implementation of data classification and access control mechanisms to ensure sensitive data is only accessible by those with proper authorization is required. Government should incorporate security considerations at the design phase of all smart economy systems. This includes performing security assessments, threat modeling, and code reviews during the development process. Besides, implementation of continuous monitoring and threat detection mechanisms to identify and respond to emerging threats in real-time. Intrusion detection systems, security information and event management (SIEM) solutions, and behavior analytics can be useful. The government must collaborate with industry peers, other governmental organizations, and cyber security experts to share threat intelligence and best practices. Building a collaborative ecosystem can help anticipate and mitigate potential threats. A smart economy's success depends on its ability to leverage technology effectively while safeguarding against cyber threats. By implementing a robust cyber security strategy that covers both digital and physical aspects, organizations can help create a secure and resilient environment for their operations within the smart economy.

5.3 Security for Smart Government

Transparent governance, social services, public services, policy and strategy development, and decision-making are all related to governance. Smart governance can be defined as the delivery of public services to citizens and other residents of a nation or region via electronic communications tools like computers and the Internet. Through smart governance, new opportunities are opened up for direct delivery of services to citizens as well as more comfortable and direct access to government services. Digital interactions between citizens and their governments (C2G), governments and other government agencies (G2G), citizens and governments (G2C), employees and firms and commerce (G2E), and governments are referred to by this term (G2B). In an effort to build a smart country, the government of Bangladesh has already begun to move toward e-governance. There are numerous e-services that are shared by various government organizations. The table below displays the number of e-Services that fall under each category.

Category	Num.	Category	Num.
Admission	28	Online Application	100
Agriculture	21	Online Registration	22
Ask Your Question	9	Passport, Visa, and Immigration	7
Digital Center	1	Postal and Courier	3
Directory	20	Radio, TV news	7
Education	29	Recruitment	12
Exam Results	8	Ticket Booking and Purchase	11
Finance and Trade	34	Training	10
Fisheries and Livestock	5	Treasury Invoice	1
Forms	3	Utility bills	11
Health Services	9	Vehicle Services	8
Income Tax	7	**Total**	**365**

Table1: The breakdown of e-Services available in Bangladesh

These services can benefit people by improving both their financial status and quality of life. However, while using these services, beneficiaries need to share their personal information. If the provided information is leaked, the users might fall in grave danger. So, cyber security for smart countries is crucial to ensure the safety, privacy, and functionality of the various interconnected systems and devices that make up these technology-based environments. For implementing the idea of smart Bangladesh, the government must identify potential threats and vulnerabilities specific to smart country systems, such as IoT devices, communication networks, data centers, and control systems and develop a comprehensive cyber security strategy that encompasses prevention, detection, response, and recovery plans. Furthermore, securing a smart country is an ongoing process that requires collaboration among various stakeholders, including city planners, technology vendors, cyber security experts, and residents. By adopting a holistic approach to cyber security, smart countries can mitigate risks and ensure a safer and more resilient urban environment.

5.4 Cyber Security for Smart Society

Globally, the smart society movement is emphasized in parallel with advancements in digital technology. The majority of research on the "smart society" focuses on how technology supports human endeavors, particularly in cities. However, with the advancement of technology, related threats are also increasing. Statistics shows that almost 5000 websites around the world are compromised each month due to cyber-attack. According to research, the most frequent reasons for data breaches are: back doors, application vulnerabilities, malware, social engineering, weak or stolen credentials, passwords, excessive permissions, insider threats, incorrect configuration, and user error. A society must conduct all of its operations sensibly in order to advance, but in the present era, cybercrime has grown so dangerous that it is affecting children, adolescents, and students. Video games, pornography, and social media scandals have become recognized as social evils. The Smart Bangladesh plan's implementation will be doubtful if the virtual world cannot now be made socially safe. So, cyber security is of paramount importance in creating and maintaining a safe and secure smart society. Government should, promote cyber security awareness among citizens, businesses, and government entities and offer training programs and resources to help people understand potential threats and best practices for staying safe online. Moreover, creating a secure smart society requires a multi-faceted approach involving technology, policies, regulations, and active collaboration among various stakeholders. By implementing these strategies, it's possible to mitigate risks and create a safer environment for individuals, businesses, and communities in a connected world.

VI CONCLUSION AND RECOMMENDATIONS

From the findings of the reviewed literatures, it can be said that cybersecurity is of paramount importance in building a smart Bangladesh for several reasons. As Bangladesh transitions towards becoming a smart nation, it will increasingly rely on digital infrastructure to manage essential services such as energy, transportation, healthcare, and finance. Ensuring the security of these critical systems is imperative to safeguard against cyber threats that could disrupt services and cause widespread harm. Besides, Smart technologies generate vast amounts of data, including sensitive personal information. Protecting this data from unauthorized access, theft, or misuse is essential to maintain public trust and comply with privacy regulations. Cybersecurity measures such as encryption, access controls, and data anonymization are crucial for safeguarding individual privacy rights.

Cyberattacks can result in significant financial losses for businesses and the economy as a whole. The costs associated with data breaches, theft of intellectual property, and disruption of operations can be substantial. Investing in cybersecurity measures will help mitigate these risks and preserves the economic stability and growth of Bangladesh. In addition to economic considerations, cybersecurity is also essential for national security. Cyber threats, including espionage, sabotage, and cyber warfare, pose risks to government institutions, defense systems, and critical national infrastructure. Strengthening cybersecurity defenses helps safeguard against these threats and protects Bangladesh's sovereignty and security interests.

Embracing smart technologies and digital innovation is essential for Bangladesh's socioeconomic development. However, this digital transformation also introduces new vulnerabilities and cybersecurity challenges. By prioritizing cybersecurity initiatives, Bangladesh can foster a secure and resilient digital ecosystem that enables innovation while mitigating associated risks. In summary, cybersecurity is not only a technical necessity but also a foundational element for building a smart and resilient Bangladesh. By prioritizing cybersecurity measures, Bangladesh can harness the potential of smart technologies while safeguarding against evolving cyber threats and ensuring the trust, security, and prosperity of its citizens.

REFERENCES

Ahmed J, A., et al., (2021). A review on security analysis of cyber physical systems using machine learning. Mater. Today: Proc.

Al Dakheel, J., et al., (2020). Smart buildings feature and key performance indicators: A review. Sustainable Cities Soc. 61, 102328.

Al-Ghamdi, M.I., (2021). Effects of knowledge of cyber security on prevention of attacks. Mater. Today: Proc.

Al-Saidi, M., Zaidan, E., (2020). Gulf futuristic cities beyond the headlines: Understanding the planned cities megatrend. Energy Rep. 6, 114–121.

Atitallah, S.B., et al., (2020). Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions. Comp. Sci. Rev. 38, 100303.

Baig, Z.A., et al., (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 22, 3–13.

Barr, S., et al., (2021). Smart Cities and Behavioural Change: (Un)Sustainable Mobilities in the Neo-Liberal City. Geoforum.

BASIS, (2022), Smart Bangladesh Report.

Chatfield, A.T. and Reddick, C.G. (2019) A Framework for Internet of Things-Enabled Smart Government: A Case of IoT Cybersecurity Policies and Use Cases in US Federal Government. Government Information Quarterly, 36, 346-357. https://doi.org/10.1016/j.giq.2018.09.007

Chen, Z., (2021). Application of environmental ecological strategy in smart city space architecture planning. Environ. Technol. Innov. 23, 101684.

Chen, D., Wawrzynski, P., Lv, Z., (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. Sustainable Cities Soc. 66, 102655.

Cybersecurity Capacity Review Bangladesh, CCRB, (2018), source, file:///C:/Users/HOME/Desktop/Migration%20Article/Smart/2020-10-20-00-13-3a751045bb7027fc505e59dfda762514.pdf

Ijaz, S., et al., (2016). Smart cities: A survey on security concerns. Int. J. Adv. Comput. Sci. Appl. 7 (2), 612–625.

Jibon, A., F., (2023), Ensuring Cyber Security a Must for Building Smart Bangladesh, The daily Sun,

Khatoun, R., Zeadally, S., (2017). Cybersecurity and privacy solutions in smart cities. IEEE Commun. Mag. 55 (3), 51–59

Lee, J., Kim, J., & Seo, J. (2019). Cyber-attack scenarios on smart city and their ripple effects. 2019 International Conference on Platform Technology and Service (PlatCon), Platform Technology and Service (PlatCon), 2019 International Conference On, 1–5. https://doiorg.sdl.idm.oclc.org/10.1109/PlatCon.2019.8669431

Lim, C., Cho, G.-H., Kim, J., (2021). Understanding the linkages of smart-city technologies and applications: Key lessons from a text mining approach and a call for future research. Technol. Forecast. Soc. Change 170, 120893

Maruf, M.H., et al., (2020). Adaptation for sustainable implementation of smart grid in developing countries like Bangladesh. Energy Rep. 6, 2520–2530

Prothom-alo (2023)-0119, "Smart Bangladesh to be built by 2041: PM".

Qamar, T., & Bawany, N. Z. (2020). A Cyber Security Ontology for Smart City. International Journal on Information Technologies & Security, 12(3), 63–74.

Secinaro, S., et al., (2021). Towards a hybrid model for the management of smart city initiatives. Cities 116, 103278.

Sengan, S., V., S., Nair, S. K., V., I., J., M., & Ravi, L. (2020). Enhancing cyber–physical systems

with hybrid smart city cyber security architecture for secure public data-smart network. Future Generation Computer Systems,112, 724–737. https://doiorg.sdl.idm.oclc.org/10.1016/j.future.2020.06.028

Vitunskaite, M., et al., (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Comput. Secur. 83, 313–331.

Witanto, J. & Lim, H., & Atiquzzaman, M. (2018). Smart government framework with geo-crowdsourcing and social media analysis. Future Generation Computer Systems. 89. 10.1016/j.future.2018.06.019.