OPEN ACCESS
Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

Recent Advancement of Cyber Security: Challenges and Future Trends in Bangladesh

Major Muhammad Masudur Rahaman[1*]

[1]Signals, Bangladesh Army

DOI: 10.36348/sjet.2022.v07i06.002 | **Received:** 16.05.2022 | **Accepted:** 01.07.2022 | **Published:** 06.07.2022

***Corresponding author:** Major Muhammad Masudur Rahaman
Signals, Bangladesh Army

Abstract

The massive demand for global transformations describes the necessity of high-speed communication in the twenty-first century. Almost every facet of online networks is changing, including international relations, politics, trade, and security. However, cyber security has become a major issue all around the world. Bangladesh has recently taken the required steps to address the problem as swiftly as feasible. In order to prevent and combat cyber threats, the government of Bangladesh plans to establish a specialized computer incident response team (CIRT) for banks and financial institutions, which will serve as the national response team responsible for receiving, reviewing, and responding to computer security incidents and activities in Bangladesh. Implementing strong and multilayer authentication to better management of the data, as well as discovering and mapping out security issues, some major initiatives are required to implement cyber security. Engineers should obtain hands-on training in decoding corrupted data files during any cyber-attack in order to recover data from any lost data. In this review, cyber security challenges in smart cities and smart governance have been examined, with an emphasis on e-commerce, machine learning, industry automation, IoT, and other security elements. The main cyber security concerns are discussed in order to better comprehend almost every necessity of long-term cyber security situations. Moreover, smart industry control and its security infrastructure, problems for implementation in Bangladesh and recent security issues have been highlighted.

Keywords: E-commerce, machine learning, smart city, Cybercrime, Cyber security, Warfare.

1. INTRODUCTION

Cyber security has become a prominent study topic as a result of the rapid expansion of digital technology in modern countries around the world. Modern life is inextricably linked to information and communication technologies (ICT). With the rapid rise in the digital technology revolution [1], the ICT division is playing a vital role in business and government. The government provides timely services to their residents using modern technology and the internet. Furthermore, with a big number of the current population, Asia may become the primary center for many investors to conduct business in areas such as banking, transportation, e-commerce, telecommunications, and shipping as a method of material and production, boosting the region's economy in the near future. The rise of decentralized data has had a positive impact on society. If there is no monitoring, cybercriminals may steal government data, including classified information [2]. This can pose a hazard to countries that are targeted by terrorist attacks or conflicts as a result of cyber-attacks. Since the beginning of the technology era in IR 4.0, information regarding internet security has been shared and debated to refresh knowledge on a regular basis. To attain this goal, more work must be done to address the issue of digital integration across the world [3]. A cyber attacker uses techniques like phishing, spam messages, and distributed denial-of-service attacks (DDoS) to harm the data environment and

[1] Staples, M., & Niazi, M. (2007). Experiences using systematic review guidelines. Journal of Systems and Software, 80(9), 1425-1437.

[2] C. T. Dai, (2015). Cyber security in Vietnam: Formulation and Implementation of a New Strategy. Herodote, 157(2), 126-140.

[3] T. V. Paul., Morgan, P. M., & Wirtz, J. J. (Eds.). (2009). Complex deterrence: Strategy in the global age. University of Chicago Press.

proactively monitor the system, making it necessary to plan continuous monitoring strategies [4]. To deploy such monitoring strategies globally, there is a rapidly increasing demand for security professionals. However, there is a shortage of skilled domain experts, which highlights the need for wider awareness and relevant undergraduate courses. With the help of cloud computing, easy access to remote services can be provided for training courses in cyber security. While such courses are becoming common, adequate training requires tutors with hands-on skills from the industry.

Modern technology is looking for a smart city where physical infrastructure, information technology facilities, social infrastructure, and commercial infrastructure are all integrated to boost the city's collective intelligence. Smart cities are massive, complex, and reliant on technology that faces a slew of technological, economic, political, and social difficulties [5]. Smart cities face difficulties and obstacles such as economic and investment problems, people's ever-changing needs, stakeholder involvement, user-friendly jointing, and safety and security. Good government, smart people, smart economics, smart transportation, environment, and lifestyle are the six major elements of a smart city [6].

The purpose of this review is to emphasize the importance of cyber security responses to these new and complex threats. The purpose is to give industry and academics a more comprehensive view of current industry security trends, as well as to aid in the engagement of appropriate security analysis, threat and vulnerability identification, and prioritizing of control/mitigation operations for effective security assurance. This begins with a thorough grasp of security concerns and dimensions, which will guide the creation of effective security solutions. Understanding developing and evolving security risks and vulnerabilities will help stakeholders gain a better understanding of security threats and vulnerabilities, as well as progress the creation of appropriate security systems. This article also examines the developing and expanding cyber security difficulties in the modern industrial arena by outlining specific concerns that provide security risks and vulnerabilities, and repercussions to various relevant businesses in Bangladesh.

The discussion on major cyber security issues is provided to better understand almost every requirement of sustainable cyber security environments. Moreover, this paper covers the security issues of emerging technologies such as smart cities, smart grids, smart energy grids, and smart intelligence transportation system (ITS). The rest of the paper is organized as follows. Section 2 contains a discussion of cyber security in Smart Governance, healthcare, smart energy systems, intelligent transportation system (ITS), and smart building technology. Cyber security Applications in e-Banking, e-Governance, and e-commerce training in Bangladesh are highlighted in sec 3, 4 and 5 Cyber culture in Bangladesh is given in section 6, and applications of cyber security such as in big data, IR4.0, and machine learning are described in section 7. Section 8 discusses Cyber Security Features and Critical Infrastructure such as infrastructure security, Cloud security, Database security, IoT security. Basic Problems of Cyber Security and Recent Challenges of Cyber Security have been elaborated in sections 9 and 10. Cyberspace acts like a Field of Warfare has been explained in section 11 and finally, the paper is concluded in Section 12.

2. CYBER SECURITY RELATED ISSUES

2.1. Smart City

Most cities have become smarter and more technologically advanced in recent years. Cities can make much better use of their infrastructure, save money, and deliver better services to their inhabitants by combining modern technology with rapid and easy communications [7]. To attract new residents, and visitors, smart cities are focusing more on providing a high quality of life and a dynamic economic condition [8]. While restricted budgets, few resources, and out-date systems usually Governments have survived to implement their objectives, innovative technologies can transform such difficulties into chances [9]. According to (Chen *et al*, 2021), the benefits of a system that automates and modifies municipal activities in order to improve citizens' lives. Smart Cities can make better use of their resources, save money, and deliver better services to their inhabitants by combining modern technology with rapid and easy communications. A smart city is concentrating more on offering a good quality of life and a dynamic economic situation in

[4] T. V. Paul., Morgan, P. M., & Wirtz, J. J. (Eds.). (2009). Complex deterrence: Strategy in the global age. University of Chicago Press.

[5] Al-Saidi, M., & Zaidan, E. (2020). Gulf futuristic cities beyond the headlines: Understanding the planned cities megatrend. Energy Reports, 6, 114-121.

[6] Razmjoo, A., Østergaard, P. A., Denai, M., Nezhad, M. M., & Mirjalili, S. (2021). Effective policies to overcome barriers in the development of smart cities. Energy Research & Social Science, 79, 102175.

[7] Lebrument, N., Cédrine Z. L., Corinne, R., & Thomas, J. R. (2021). "Triggering participation in smart cities: Political efficacy, public administration satisfaction and sense of belonging as drivers of citizens' intention." Technological Forecasting and Social Change 171, 120938.

[8] Thornbush, M., & Oleg, G. (2021). "Smart energy cities: The evolution of the city-energy-sustainability nexus." Environmental Development 39, 100626.

[9] Secinaro, S., Valerio, B., Davide, C., & Paolo, B. (2021). "Towards a hybrid model for the management of smart city initiatives." Cities 116, 103278.

order to attract money, new inhabitants, and visitors [10]. Moreover, smart parking, structured health consciousness, immediate urban noise monitoring, traffic control, lane optimization, and smart lighting is also providing a smart lifestyle [11]. The Internet of Things (IoT) is a live technology that is employed in the smart city components stated above. On the other hand, the cloud system is a live platform for storing and analyzing centralized smart city data, where cyber security is the most concern subject [12].

2.2 Smart Government

By integrating ICT for planning, administration, and operations in a single layer or across levels, the smart government creates value for long political production. To put it another way, smart government is the use of information and communication technology in business operations that provide information continuity between the government and the provision of high-quality services. The next phase in e-government is smart governance [13]. By boosting situational awareness, delivering effective and appropriate responses, and investigating incidents using real-time data, smart government decreases crime and improves city services [14]. To establish a smart government, cyber security is the most essential part which will lead to a state in front.

2.3 Smart Healthcare

Smart healthcare is a sort of health care that uses technology like wear ables, the IoT, and mobile Internet to constantly link individuals, health facilities, and organizations. Finally, it actively controls the ecosystem's demands and responds to them effectively [15]. Physicians, patients, hospitals, and medical research institutes are the core components of smart healthcare. Disease prevention, patient monitoring, diagnosis and treatment, hospital management, health decision-making, and medical research are all examples of intelligent health care. The ability to remotely monitor smart devices is made possible by wirelessly connecting them. The process in a smart city equipped with smart healthcare is described in Fig. 1, where cyber security is the heart of the system [16].

2.4 Smart Energy System

Traditional electricity grid infrastructure is insufficient to satisfy the requirements of expanding communities. A smart and contemporary energy grid is required to meet the demands for dependability, scalability, environment-friendly energy generation, and cost-effectiveness [17]. A smart energy grid using IC technology solutions can provide two-way communication and electrical currents between distinct entities in the grid (see Fig. 2) [18]. Real-time monitoring is possible with the smart grid, ensuring the most efficient power exchanges between the power grid and clients. Moreover, it also enables the creation of environmentally friendly power by incorporating renewable energy sources into the system on both the Power Company's and the customers' sides [19,20]

[10] Ma, C. (2021). "Smart city and cyber-security; technologies used, leading challenges and future recommendations." Energy Reports 7, 7999-8012.

[11] Nakano, S., & Ayu, W. (2021). "Will smart cities enhance the social capital of residents? The importance of smart neighborhood management." Cities 115, 103244.

[12] Qayyum, S., Fahim, U., Fadi, A. T., & Mohammad, M. (2021). "Managing smart cities through six sigma DMADICV method: A review-based conceptual framework." Sustainable Cities and Society 72, 103022.

[13] Chatfield, A. T., & Christopher G. R. (2019). "A framework for Internet of Things-enabled smart government: A case of IoT cyber security policies and use cases in US federal government." Government Information Quarterly 36(2), 346-357.

[14] Witanto, J. N., Hyotaek, L., & Mohammed, A. (2018). "Smart government framework with geo-crowdsourcing and social media analysis." Future Generation Computer Systems 89, 1-9.

[15] Wang, W., Haiping, H., Fu, X., Qi, L., Lingyan, X., & Jiansheng, J. (2021). "Computation-transferable authenticated key agreement protocol for smart healthcare." Journal of Systems Architecture 118, 102215.

[16] Mohanty, S. P., Uma C., & Elias, K. (2016). "Everything you wanted to know about smart cities: The internet of things is the backbone." IEEE Consumer Electronics Magazine 5(3), 60-70.

[17] Kourgiozou, V., Andrew, C., Mark, D., Dimitrios, R., & Dejan, M. (2021). "Scalable pathways to net zero carbon in the UK higher education sector: A systematic review of smart energy systems in university campuses." Renewable and Sustainable Energy Reviews 147, 111234.

[18] Ahmad, T., & Dongdong, Z. (2021). "Using the internet of things in smart energy systems and networks." Sustainable Cities and Society 68, 102783.

[19] Australian Cyber Security Centre, https://www.cyber.gov.au/, Accessed on Jan. 10, 2020

[20] Mehrpooya, M., Noradin, G., Mohammad, M., & Sohrab, A. G. (2021). "Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device." International Journal of Energy Research 45(11), 16436-16455.

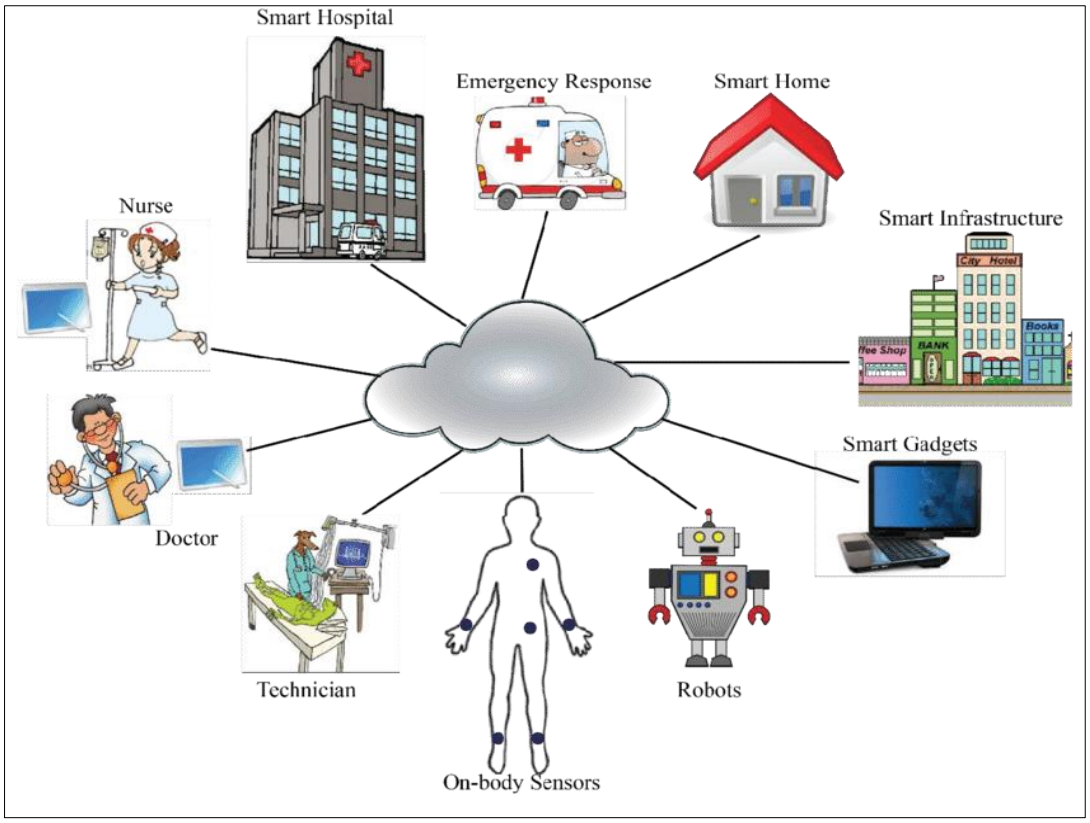

Fig. 1 The process in a smart city equipped with smart healthcare (Mohanty, 2016)

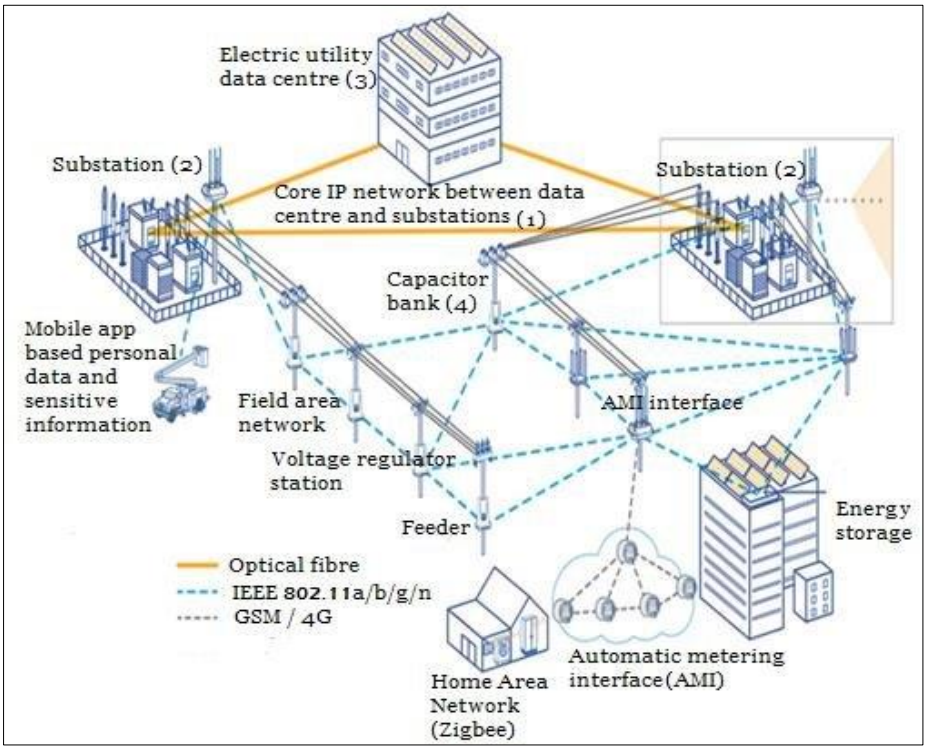

Fig: 2 Smart grid: An IoT-based electricity generation, transmission, and distribution network containing automated operation data [2]. Source: Avishek Gupta [2019]

2.5 Smart Intelligence Transportation System (ITS)

The effective utilization of existing infrastructure and current technologies is one of the planners' priorities in modern traffic management systems. One of the ultimate goals of traffic control systems in this sector is to boost network efficiency while also improving vehicle safety and reducing journey time. To achieve the aforementioned aim, the

transportation network provides efficient transportation service systems and also skilled system administration [21]. The most significant benefits of implementing smart transportation systems include reduced traffic congestion, increased safety, and time savings, reduced fuel consumption, and improved service. The system's key components include compliance monitoring and recording systems, a climatic status information system, a driver warning system, and a vehicle information system, as well as the convenience of quick and efficient police enforcement and an increase in social security. Active road safety to enhance road safety, location-based services to improve location-based services, and worldwide internet services to improve global internet services are the four categories of smart transportation systems. The next step is to think about cyber security issues for implementing smart ITS.

2.6 Smart Building Technology

Sensors and grid technologies are used in smart buildings to interact with building equipment, the report recorded energy usage to the smart grid through a smart meter, and allows data to be transferred from the smart grid to the building. Building owners will be able to remotely monitor and these buildings will be able to adjust their energy patterns based on smart grid features [22]. The smart building's connectivity to the smart grid enables the smart grid to achieve some of its primary objectives. Demand response, effective feedback, peak shaving, and energy exchange are just a few of the advantages of this link [23]. The smart building platform is made up of two components: building operational technology and external information (See Fig. 3) [24].

3. Cyber Security in Smart e-Governance

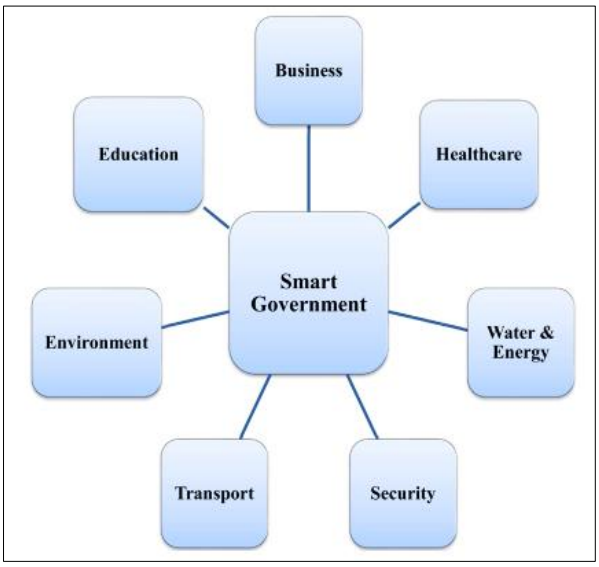

Fig 3: Key concepts of Smart Governments

Cyber-security protects computers, networks, mobile phones, and electronic systems against hostile assaults, and its role may be defined as follows: protecting people's devices, data stored on those devices, and the identities of individuals who utilize that data [25]. Businesses are exploring to protect the lack of cyber security that is exposed to data breaches and hacker attacks, making them ideal targets for cybercriminals. As a result of the globalization of communications and the usage of cloud services to store personal data, security issues are developing [26]. Cyber-attack and Cyber-terrorism are a type of terrorism that aims to frighten people by damaging electronic systems or intentionally hacking others' information [27]. Key concepts of smart Governments are described in Fig 3.

Other terms "PC banking," or "Internet banking," "Telephone banking," and "mobile banking" refer to a multitude of ways for customers to access their bank accounts without having to manually visit a branch. E-banking is a term that refers to all types of electronic banking transactions. Telebanking is a

[21] Jeong, H. H., Yiwen, C. S., Jaehoon, P. J., & Tae, T. O. (2021). "A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications." Vehicular Communications 31,100349.

[22] Mehrpooya, M., Noradin, G., Mohammad, M., & Sohrab, A. G. (2021). "Numerical investigation of a new combined energy system includes parabolic dish solar collector, Stirling engine and thermoelectric device." International Journal of Energy Research 45(11), 16436-16455.

[23] Aborokbah, M. M., Saad A. M., Arun, K. S., & Oluwarotimi, W. S. (2018). "Adaptive context aware decision computing paradigm for intensive health care delivery in smart cities—A case analysis." Sustainable cities and society 41, 919-924.

[24] Al Dakheel, J., Claudio, D. P., Niccolò, A., & Fabrizio, L. (2020). "Smart buildings features and key performance indicators: A review." Sustainable Cities and Society 61, 102328.

[25] Olabumuyi, O., Obioma, U., Ebunoluwa, A., & Olawale, A. (2021). "350 Perception of Nigerian women on violation of Traditional Gender Role-related IPV." International journal of epidemiology, 50(1), 168-510.

[26] Alhayani, B. SA. (2021). "Visual sensor intelligent module-based image transmission in industrial manufacturing for monitoring and manipulation problems." Journal of Intelligent Manufacturing 32(2). 597-610.

[27] Huang, A., Ruoping, L., Vladimir, E., Serguei, T., Krtin, K., & Vadim, M. (2020). "Laser-damage attack against optical attenuators in quantum key distribution." Physical Review Applied 13(3), 034017.

banking service that is provided over the phone. To gain access to the system, call a certain phone number that provides a variety of services. There are two types of computer banking. The first one is internet banking, which is sending and receiving money through secure networks. The second group includes Internet banking, which has been available in Germany since the mid-1990s, but it was the sole product available at the time of data collection. Internet banking allows clients to do transactions from any terminal with Internet access. Both bankers and clients would no longer need proprietary software to execute online banking transactions if they used internet banking. Financial service providers face considerable challenges as a result of these circumstances. As a result, the Internet is now seen as a "strategic weapon" for addressing ever-changing client expectations and innovative enterprise needs. Layers of protection from the network to the browser are included in the comprehensive security architecture, as well as effective encryption that protect consumers from penetration when they contact the bank via the public network. Mobile banking is similar to online banking. Mobile banking is a great example of how the lines between different forms of e-banking are becoming increasingly blurred. WAP, mobile phones, personal digital assistants (PDAs), and tiny hand-held PCs are providing bank clients with Internet access, paving the door for Internet banking. It offers a high level of flexibility and allows financial services to operate regardless of time or place.

4. E-Banking issues in Bangladesh

Mobile banking is still in its development stage in Bangladesh. With the use of information technology, the banking industry has experienced substantial changes in the way its services customers. As a consequence of developments in IT and telecommunications, Bangladesh's banking sector is undergoing an electronic revolution. Foreign Commercial Banks (FCBs) in Bangladesh are leading the way in introducing modern financial goods and services. PCBs (Private Commercial Banks) are starting to follow suit. Nationalized Commercial Banks (NCBs) such as Sonali, Rupali, Janata, and Specialized Banks (SBs) have yet to achieve notable success in these sectors. They are currently developing innovative and unique products and services in response to the demands of the customers. The majority of Bangladeshi banks now provide offer electronic products and services. Because they offer some of the important aspects of e-banking, such as intra-bank transactions, letters of credit (LC), and money markets. Traditional banking products and services are separated into two groups such as traditional banking products and contemporary and innovative banking services, commonly which are known as E-banking.

5. Security Concerns in E-Commerce of Bangladesh

Online transactions in e-commerce, online banking activities, and the use of mobile financial services (MFS) have increased across the country as a result of repeated lockdowns caused by Covid-19. During the epidemic, MFS has shown to be one of the most reliable methods of disbursing funds under the government's numerous incentives and social security programs. Various private enterprises, particularly the garment industry, have used such systems to pay salaries and bonuses. However, the increasing adoption of new technologies raises the issue of cyber security. Despite its enormous potential, Bangladesh's e-commerce industry is affected by problems such as discrepancies between real products and those depicted on e-commerce sites, delays in customer delivery, a lack of reliability and validity, inconvenient return policies, limited online payment options, and limited cash on delivery options (2013, Chavan). According to BTRC data from 2012 to 2016, the total number of internet subscribers in Bangladesh was 30.48 million in 2013, 56.17 million in 2016, and 120.95 million in 2021. The current annualized volume of e-commerce is estimated to be USD 100 million, according to IBIS World, with seasonality peaks during yearly religious holidays. According to the data above, e-commerce in Bangladesh has tremendous potential if it can reach the masses through a suitable delivery route. Commissions on product selling, shipping costs, product profit, and restaurant commissions are all ways that the e-commerce industry generates money (UNCTAD, 2015). Supervisors, as well as persons and software, are used as part of the monitoring system. Maintaining a distribution channel needs, among other things, the employment of one's own vehicle, employees, and third-party participation. Despite the fact that e-commerce is an internet-based business, the majority of e-commerce enterprises have yet to be able to distribute things across Bangladesh. For client satisfaction feedback, the majority of e-commerce enterprises rely on website ratings and Facebook reviews. The Facebook, campaign, fest participation, tempting prices, news publications, and offline campaign are some of the most frequent marketing techniques for e-commerce firms in Bangladesh [28].

6. Cyber Culture in Bangladesh

Internet users in Bangladesh too often “blindly” trust ICT and traditional internet services structure of the applications they use. It did not become clear from the consultations to which extent the government offers e-services. A different picture was revealed with respect to e-commerce services, which have become very popular in the country over the years, making it one of the booming sectors in Bangladesh (such as Uber). The trust levels of e-commerce services have increased because of the quality of the services

[28] Islam, M. S., & Sharmin, A. E. (2018)."Electronic commerce toward digital Bangladesh: Business expansion model based on value chain in the network economy." Romanian Economic and Business Review 13(3), 7-19.

experienced since they have been offered. Despite the proliferation of e-commerce services, the suppliers have not yet recognized the need for the application of security measures. People in Bangladesh have little or no understanding of how personal information is handled and the protection of personal information online. There are two main institutions as National CSIRT and the police from the public sector for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents. Victims can go to the police or to a special branch to launch a complaint or contact the cyber call desk via phone, email, or online portals.

Cyber incident has been shown in Fig. 4

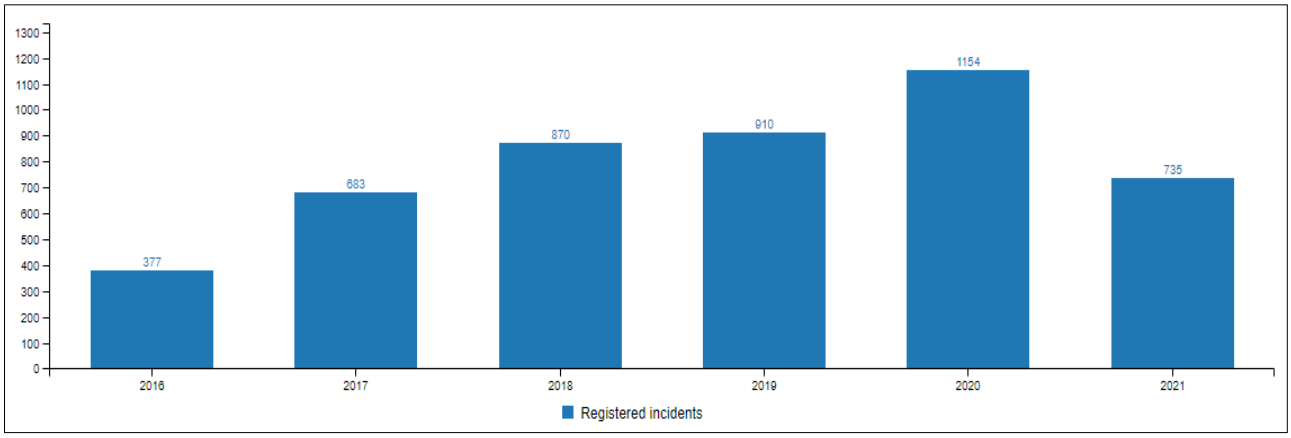

Fig 4: Cyber incident in Bangladesh per year [i] [Dhaka tribune, June, 21]

Awareness-raising programs are available but they are very ad-hoc and especially for different target groups. The BGD e-GOV CIRT as part of BCC engages in the design of awareness campaigns and has adapted some of the Stop. Connect materials and publishes material on its website but it was not clear from the consultations if they are targeted to specific target groups and if any metrics were applied. Participants also mentioned there were a number of initiatives supported by international partners. The government has not yet realized the action item of the NCS and a coordinated National Cyber security Education Framework. Despite the government taking different initiatives to introduce cyber security qualification programs and to increase the number of cyber security experts, both are still very limited. The need for training professionals in cyber security has been documented in the current NCS [[29]] (CIRT, 2021). However, there was also no evidence from the consultations to the extent initiatives were implemented. In the private sector, cyber security training is mandatory in some industries but for instance in the finance sector, educational institutions, and training institutes. Participants emphasized the need to develop a national framework and procedures to implement cyber security frameworks across organizations regarding skills development. If an organization finds no activity, they should apply available patches immediately and implement the mitigations in this Alert. HAFNIUM exchange servers implemented by Cyber threat research unit, BGD e-GOV CIRT CISA. BGD e-Gov CIRT is constantly doing vulnerability assessments and penetration testing on assets located at the National Data Center as well as these activities can be provided to the constituency on a special official request.

7. Cyber security Applications

BGD e-Gov CIRT is developing Cyber security related Policies, guidelines framework, standards, controls, and guidelines. Distributing them to relevant authorities, providing training and monitoring on a regular basis.

7.1 Cyber Security in Big Data

In today's digital era, the ancient saying "knowledge is power" has been shown to be accurate. Having access to information leads to knowledge. The capacity to extract information from vast amounts of data has become a significant challenge. Researchers created the phrase "big data analytics" to define the art of processing, storing, and accumulating huge volumes of data for future analysis. The amount of data being created is annoying. The Internet's fast expansion, as well as the Internet of Things (IoT) is the primary drivers of this long-term growth. The term "big data" has become a catchphrase for the production of huge amounts of data. Massive amounts of data are being produced at an alarming rate. Cloud computing, on the other hand, still carries a number of dangers. In this case, confidentiality refers to the safeguarding of data against unwanted access or use. The prevention of illegal and incorrect data change would be considered integrity. Data availability includes data recovery from hardware, software, and system failures, as well as data access rejections. When it comes to protecting large data, privacy is the most crucial factor. Access control and encryption are two of the most well-known data privacy solutions. The most common methods for large

[29] https://www.cirt.gov.bd/about-us/

data security were encryption and access control. Other techniques, which may or may not require some sort of encryption, have been attempted by researchers. Because of the nature of massive data, it's tough to keep anything safe. Some academics have attempted to identify the most critical aspects of large data in order to safeguard it. M. R. Islam (2017) proposed a system for classifying data based on a person's societal value and evaluating the data's sensitivity levels in order to address the issue of protecting personal health records. Furthermore, (R. Achana, R, 2015) attempted to secure the most important/valuable properties of large data because safeguarding everything is a tough undertaking. To safeguard these high-value characteristics, they utilize data masking. They employ a ranking system that prioritizes for large data security to decide which ones are valuable. The authors provided an attribute selection technique for protecting the value of big data by using a ranking algorithm to find higher-importance features and applying security protocols. They focused on the characteristics of big data and provided a security hardening strategy that relies on attributes to protect massive data sets [30].

7.2 Cyber Security for Industry Revolution 4.0

Industry 4.0 changes, according to management consulting company McKinsey & Company, have the potential to generate value comparable to 15 to 20% efficiency gains [31]. Additionally, the capacity to evaluate vast volumes of data created by industrial activities offers a number of benefits. According to Cisco's 2018 Annual Cyber Security Reports [32], 31% of businesses have suffered cyber-attacks against Operational Technology (OT), with 38% expecting assaults to spread from Information Technology to OT. Despite the fact that 75% of experts believe Cyber Security is a top concern, just 16% believe their organization is well equipped to tackle cyber security threats [33].

7.3 Cyber Security in Machine Learning (ML)

To offer security by drawing actionable insights from data, machine learning algorithms are required. There are three types of machine learning algorithms: supervised learning, unsupervised learning, and semi-supervised learning (which are a combination of supervised and unsupervised learning). The outcome of each training sample is unknown, unsupervised learning techniques are utilized. Malware detection is a good example. Clustering methods and Principal Components Analysis are commonly employed for unsupervised learning malware analysis (PCA). Linear and regression analysis, support vector machines, regression trees, and neural networks, all of which have been rebranded as deep learning, are some of the techniques used for classifiers. Deep learning algorithms are highly good for evaluating vast volumes of unsupervised data with a lot of diversity; therefore, they have a lot of promise when it comes to analyzing network data for intrusion detection, especially for NIDS [34]. Reference [35] tackled this issue when they used a deep learning technique called Self-taught Learning (STL) on the NSL-KDD dataset. Deep learning, on the other hand, faces certain difficulties with huge data [36]. When attackers target Machine Learning models, their flexibility might be leveraged as a weakness. Antagonistic examples are machine learning inputs that are intended to deceive the ML model into generating a different result. Machine learning (without human interaction) can collect analyze and prepare data. In cyber security, this innovation makes a big difference to analyze past cyber-attacks and create individual defense reactions.

Various studies in this field have attempted to improve the models. On the other hand, proposes a new method for detecting hostile cases [37]. This method is known as feature squeezing, and it entails condensing an adversary's search space by combining samples that match to many different feature vectors in the original space into a single sample. Attackers are leveraging artificial intelligence to get around some of the machine-learning automated procedures, thanks to the growth of Generative Adversarial Networks and large data. Instead, combining human and computer aspects

[30] Kim, S. H., Jung-Ho, E., & Tai-Myoung, C. (2013). "Big data security hardening methodology using attributes relationship." In 2013 International Conference on Information Science and Applications (ICISA), p1-2. IEEE.

[31] ISO/IEC 27032: 2012(en), Information Technology – Security Techniques – Guidelines for Cyber Security, Accessed in 2018.

[32] Ten, Chee-W., Govindarasu, M., & Chen-Ching, L. (2010). "Cybersecurity for critical infrastructures: Attack and defense modeling." IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4), 853-865.

[33] Official Website of the Department of Homeland Security, 2020.https://www.dhs.gov/topic/cybersecurity

[34] Cardenas, A. A., Saurabh, A., & Shankar, S. (2008). "Secure control: Towards survivable cyber-physical systems." In 2008 The 28th International Conference on Distributed Computing Systems Workshops, p.495-500. IEEE.

[35] Askoxylakis, I., Henrich, C. P., & Joachim, P. (2012). Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems: 6th IFIP WG 11.2 International Workshop, WISTP, Egham, UK, Proceedings. Vol. 7322. Springer, 2012.

[36] Zhu, B., Anthony, J., & Shankar, S. (2011). "A taxonomy of cyber-attacks on SCADA systems." In 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing, p. 380-388. IEEE.

[37] Weiss, J. (2010). Protecting industrial control systems from electronic threats. Momentum Press.

is a more successful method. Vimod [38] developed a collaborative model in which humans and machines work together. To monitor networks and network traffic, they utilized high-functioning autistic graduates with special characteristics. By following the behaviors of security analysts, this technique attempts to automatically build a data triage automaton. One of the most effective methods to counteract these threats is for humans and machines to work together.

7.4 For Industrial Control Systems

Management practices aren't as well-suited to ICS/SCADA (Industrial control system)/ (Supervisory Control and Data Acquisition) systems as they are too traditional IT. As a result, there is a gap in how ICS/SCADA systems are seen and handled between management and operations staff [39]. Some planned bad actors have figured out these potentials and vulnerabilities, and they haven't stopped using them for their evil goals [40]. Technological advancements have resulted in greater competitiveness, the introduction of monitoring in an open-linked system, and real-time information exchange [41]. These have prepared the path for more efficient electronic administration, control, and monitoring of industrial equipment, and also internetworking possibilities between corporate and industrial networks. The drawback of this integration is that it has enabled various security vulnerabilities and dangers in the industrial sector (systems and networks), allowing easy access and exploitation by hostile actors, which was not the case previously. Given the evidence of successful sabotage attacks that have had massive destructive effects on victim businesses and dependent economies, ICS security has now become a crucial concern. It is far from an option to do nothing in the face of tremendous dangers to company and operational continuity, the environment, and human safety. Threats and assaults against ICS functionality are often aimed at violating ICS-prioritized security goals (availability, integrity, and confidentiality, etc.).

8. Cyber Security Features and Critical Infrastructure

The security of a system, as well as the data it holds and maintains, is largely determined by its software. Program and application security is determined by how effectively the requirements meet the needs that the software is meant to solve, as well as how well the software is developed, built, tested, deployed, and maintained. Some programs are more vulnerable to attacks than others. Ethical issues emerge during the design, deployment, usage, and retirement of software, and the documentation is important for everyone to understand these implications. These security concerns are addressed in the Software and Application Security knowledge area. Fundamental concepts and practices make up the knowledge units in this knowledge domain. To avoid software security design problems, it's become critical to address key concepts [42]. Static and dynamic testing should be performed on implementation concerns, as well as setting and patching.

Critical infrastructure includes the electrical grid, water purification, traffic lights, and hospitals, among other cyber-physical systems that civilization relies on. While the complex infrastructure provides excellent capabilities for operation, control, management, and analysis, it also exposes it to a wide range of hazards from natural and human causes, raising the potential of a hostile cyber-attack. Flexible solutions that can adjust to their specific industrial environments and problems while still being powerful enough to keep the most dedicated or advanced attacker are required for effective security against these attacks. Physical infrastructure, such as buildings, roads, plants, and pipelines, is essential to all key infrastructure sectors. Critical businesses are increasingly reliant on cyberspace and the Information and Communication Technologies (ICTs) that enable it. The Critical Information Infrastructure (CII) manages and operates critical sectors as well as their physical assets. As a result, preserving Cyberspace's trustworthy operation is a strategic national aim, as a lack of trust and credibility in the use of ICTs might hinder everyday life, trade, and national defense.

8.1 Cloud Security

The migration to the cloud by businesses presents new security challenges [43]. In contrast, this simplifies security for organizations who outsource their data to a cloud service reducing operating costs, but it also spotlights cloud services as extremely sensitive targets for attack. The biggest issue with cloud computing is that the 'third-party' component has historically been the root of most people's aversion to using it. Many people believe that because their server is not in the same building as theirs, their data will be

[38] Ani, U. P. D., Hongmei, H., & Ashutosh, T. (2017). "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective." Journal of Cyber Security Technology, 1(1), 32-74.

[39] Johnson, R. E. (2010). "Survey of SCADA security challenges and potential attack vectors." In 2010 international conference for internet technology and secured transactions, p.1-5. IEEE.

[40] Dickman, F. (2019). "Hacking the Industrial SCADA network." Pipeline and Gas Journal 236(11).

[41] Ani, U. P. D., Hongmei, H., & Ashutosh, T. (2017). "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective." Journal of Cyber Security Technology 1(1), 32-74.

[42] Arce, I., Kathleen, C. F., Neil, D., Jim, D., Danny, D., Christoph, K., Tadayoshi, K. (2014). "Avoiding the top 10 software security design flaws." IEEE Computer Society Center for Secure Design (CSD), Tech. Rep.

[43] R. Gedda. (2016). Data manipulation, Cybersecurity – Threats, Challenges, Opportunities.

less secure. This is due to a lack of physical access to the server where their data is stored. On the other hand, data centers employ people with a more specific understanding of server and data security and safety procedures [44]. Even the most dedicated in-house team will fall short of major cloud computing companies' competence and skill level. Very few (multibillion-dollar) corporations can afford to dedicate specialized employees to server security.

8.2 Database Security

Security for all elements and components of a database is covered and enforced by database security. A database administrator or other information security expert usually plans, implements, and maintains database security. In contrast to data access security measures, which focus on the security of networks, servers, or applications, data centric security measures focus on the protection of the data itself. Database cyber security precautions include not just preventing unwanted access to database data, but also the server's and backup equipment's physical security in the event of theft or destruction. Some critical components of this sector of cyber security include implementing robust and multivariable authentication to better govern who has access to data, as well as identifying and mapping out security flaws. Load and stress testing should be undertaken to ensure the database does not crash during Distributed Denial of Service (DDoS) attacks.

8.3 Internet of Things (IoT) security

Before preventive changes can be taken, it is necessary to understand IoT security challenges and risks. The ultimate goal should be to identify assets as well as to document any threats, assaults, or weaknesses that the Internet of Things may face. Many security vulnerabilities have been uncovered, such as confidentially, privacy, and entity trust, indicating that data security concerns must be addressed. Furthermore, current research should focus more on cyber threats, which would include actors, motives, and capabilities, all of which are driven by Cyberspace's unique features.

9. Basic Problems of Cyber Security

According to recent findings published in government publications, physical and cyber-based attacks on power grids and other critical infrastructure systems are becoming more common and sophisticated. The advancement of Internet technology has created major issues, such as the necessity for a professional cyber security system to secure the system's important data. Internet technology has grown through time to deliver a wide range of tasks and services, in tandem with technological innovation and demand. The protection of the Internet and its users has become an important part of both new service policy and government protection. To reach this goal, it is suggested that the numerous dangerous products be investigated and understood. The battle against cybercrime is essential for a more complete and secures strategy. As a result, a thorough grasp of the many aspects of cyber security is required. Without a comprehensive understanding of all aspects of cyber security, any cyber defense plan would be vulnerable. Because the scope of cyber security is so vast, any successful cyber security plan must account for all of them [45]. Intentional cyber-attacks may cause massive incidents, large direct and indirect costs, and affect a corporation’s competitive position and strategic goals (Spremić M, 2013). Bangladesh must minimize "cyber risks" to a minimum in order to ensure the correct execution of military tasks. This will require a continual analysis of potential threats, as well as a management structure to detect cyber vulnerabilities and enable early identification of a cyber-attack.

Due to a lack of knowledge and awareness, it is difficult to track down the adversary in cyber security. Employees are typically the weakest link in a company's cyber security chain, and they regularly open the doors to attackers owing to a lack of awareness. To avoid cyber-attacks, technology creators must have a high level of security awareness. Some countries have policies, education, and awareness systems that are appropriate. As a result, our community has to come up with a set of rules to avoid such damaging behavior. A basic understanding of cyber threats and risks, and appropriate reaction options, are all encouraged through cyber security awareness. When citizens are exposed to cyber threats, they are educated on best practices and preventative measures. The authority should work with key participants to create and implement awareness training programs aimed at distributing knowledge about cyber threats and risks, as well as industry standards for dealing with them. Cyber risks are the work of "bad hackers" (black hats), who operate on their own or within an organized criminal group to perpetrate cybercrime when the government fails to do so. Cyber security knowledge should be fostered among the general public, enterprises, and government officials.

10. Recent Challenges of Cyber Security

Cyber security is a concern for individuals, corporations, and governments alike. One of the most difficult parts of Bangladesh’s Cyber Security issue is keeping data secure from the world when something is on the internet. Examples include ransom ware, phishing attacks, malware attacks, and other cyber security risks. Cybercrime has gained in popularity in recent years, and data show that 33 complaints were submitted to the tribunal in Bangladesh in 2014, with

[44] Kuerbis, B., & Farzaneh, B. (2017). "Mapping the cybersecurity institutional landscape." Digital Policy, Regulation and Governance.

[45] Nicho, M. (2018). "A process model for implementing information systems security governance." Information & Computer Security.

the annual number gradually rising to 1,189 in 2019. During the pandemic in 2020, 1,128 cases were filed [46]. Ransom ware is a sort of software that acquires access to a user's data and locks them out until they pay a ransom. Ransom ware assaults are awful for individuals, but they're considerably worse for organizations that can't get access to the data they need to conduct their operations. According to the Ministry of Posts, Telecommunications, and Information Technology, 49% of school children in the country will be victims of cyber bullying on a regular basis by 2021. As the number of IoT devices grows at an exponential rate, so does the threat of cyber-attack. Important user data may be jeopardized if IoT devices are hacked. Securing IoT devices is one of the most difficult topics in Cyber Security.

The majority of individuals nowadays use cloud services for both personal and professional objectives. Hacking cloud platforms to steal consumer data is also an issue in Cyber Security for organizations. The infamous iCloud breach, which exposed celebrity private photographs, is well-known. Phishing is a type of media manipulation technique that is frequently used to get sensitive information from people, such as login details and credit card numbers. The hacker does not block confidential user data after gaining access to it, unlike ransom ware attacks. Instead, they use it for personal gains, such as through online shopping and laundering. Although the phrases block chain and crypto currency may be obscure to the average internet user, companies rely heavily on these technologies. As a result, assaults on these frameworks pose major Cyber Security risks for businesses, as they may jeopardize customer data and corporate operations. Contrasting that, we found a steady decline in the spread of misinformation or fake news. The rate fell from 22.33% in 2019 to 16.31% in 2020. However, in Bangladesh, sexual harassment and revenge porn cases have increased to 7.69% from 6.05% in 2019 [47]. Organizations must be aware of the security risks connected with these technologies and guarantee that attackers cannot exploit security flaws.

11. Cyberspace as a Field of Warfare

Cyber operations have become a necessary component of modern warfare. Cyber skills are created and deployed as a force multiplier, a supplement to traditional capabilities, or as a stand-alone capability to provide a "military advantage." Cyber attacks' potential to paralyze computer networks and inflict kinetic harm on infrastructure, particularly civilian key infrastructure, is becoming more crucial in current military strategy. "The next major battle will start in cyberspace," the National Security Agency (NSA) predicts that an increasing number of countries are investing heavily in cyber warfare and forming cyber armies. Because other countries may be developing cyber-attack capabilities, that might be the start of clandestine cyber provocations. Defaulting and unstable states, as well as terrorist and criminal organizations, will try to make use of cheap software, freeware, and commercial off-the-shelf software as effective cyber to undermine the credibility of our military. In a time when defense funds are shrinking, the increase in cyber security resources leads to the conclusion that the money is being spent not just on cyber-defense but also on cyber-offensives. Whereas most countries keep their cyber warfare resources and doctrine under wraps, several have declared openly that they are spending significant sums on cyber intelligence and counterattack capabilities. Bangladesh National Defense College (NDC) and Bangladesh Bank (BB) came under state-sponsored cyber-attack on several occasions. Bangladesh Bank lost millions of dollars to cyber theft and was left vulnerable to further attacks by the same rogue nation [48]. Cyberweapons have never been deployed in a large-scale battle between equals, and the incidents that have occurred so far have not caused substantial long-term consequences. It will be difficult to estimate the true capabilities of different cyber powers until that happens.

As modern warfare migrates more and more to cyberspace, the players and their skills have shifted as well. States that are regarded weaker in terms of traditional fighting force can gain a significant asymmetric advantage because to digital technology. The cyber domain has low entrance barriers when compared to traditional security domains. As a result, cyber capabilities are increasingly being used to gain leverage in international security, undermining traditional great powers' military superiority and doctrine. Through a variety of readily available and inexpensive cyber instruments, the new toolbox of "cyber power" allows not just traditionally weaker governments but also non-state actors to exert enormous force against larger adversaries. Data breaches, advanced cyber espionage, and cyber-generated physical attacks can all be caused by malicious code and expertise that can be purchased or rented.

[46] Cybercrime cases rise in Bangladesh, https://bdnews24.com/bangladesh/2021/09/06/cybercrime-cases-rise-in-bangladesh

[47] Research on Cyber Crime Trends in Bangladesh-2021, https://ccabd.org/research-on-cyber-crime-trends-in-bangladesh-2021/

[48] Bangladesh National Defense College, https://archive.dhakatribune.com/opinion/op-ed/2017/12/17/cyber-warfare-achilles-heel

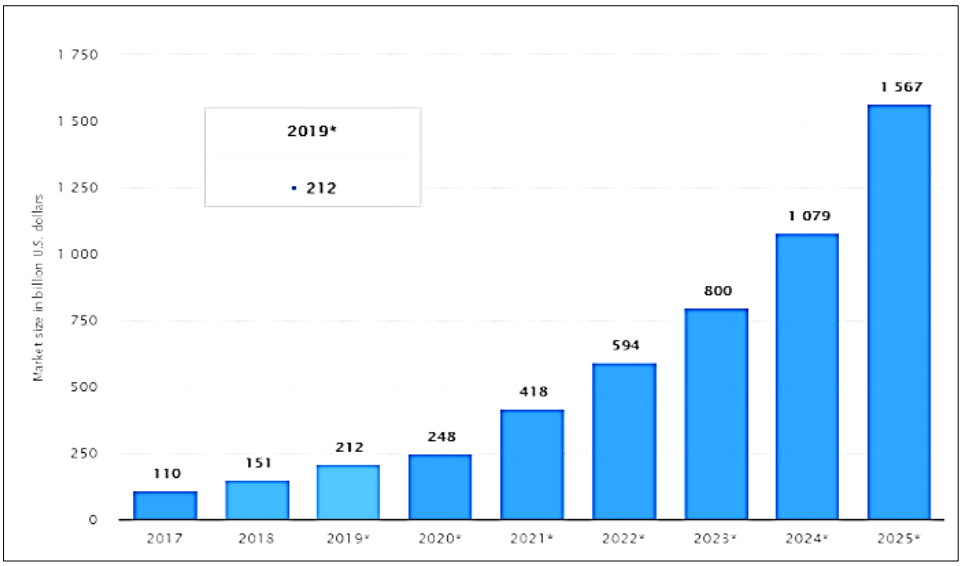

Fig 6: IoT market size expected until 2025 [ii]

12. CONCLUSION

Cyber security is a never-ending battleground. While the inherent nature of IT, the complexity of information technology systems, and human fallibility are the root causes of most cyber security vulnerabilities, a lasting solution will not be developed in the near future. When new defenses are introduced to tackle prior dangers, intruders adapt by developing new tools and methods to attack security. New IT applications develop, criminals, terrorists, and other hostile parties gain new possibilities, as well as new weaknesses that bad actors may exploit. The approaches for adapting modern, state-of-the-art security measures for cyber threat prevention and mitigation mechanism should be implemented. To detect and verify cyber threats efficiently, correct system components must be implemented while taking into account the cyber security lifecycle and following standards and best practices. Real-world examples from a range of industries, including, but not limited to, industrial controls systems, smart grids, and smart cities, have been used to study the potential repercussions of cyber threats. Traditional cyber security research focuses on refining existing technology and procedures as well as inventing completely new cyber security techniques. New cyber security technologies, methods, tactics, organizational structures, and other data will help to strengthen defenses against a constantly changing threat.

BIBLIOGRAPHY

- Agrafiotis, I., Giniotienė, A., & Weisser Harris, C. (2018). Cybersecurity Capacity Review Bangladesh.
- Amalina, F., Hashem, I. A. T., Azizul, Z. H., Fong, A. T., Firdaus, A., Imran, M., & Anuar, N. B. (2019). Blending big data analytics: Review on challenges and a recent study. *Ieee Access*, *8*, 3629-3645.
- Faria, R., Brito, L., Baras, K., & Silva, J. (2017, July). Smart mobility: A survey. In *2017 International conference on internet of things for the global community (IoTGC)* (pp. 1-8). IEEE.
- Islam, M. R., & Ahmad, M. (2019, February). Wavelet analysis based classification of emotion from EEG signal. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)* (pp. 1-6). IEEE.
- Macaulay, T., & Singer, B. L. (2011). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press.
- Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, *5*(3), 60-70.
- Njoh, A. J. (2018). The relationship between modern information and communications technologies (ICTs) and development in Africa. *Utilities Policy*, *50*, 83-90.
- Rymarczyk, J. (2020). Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. *Entrepreneurial business and economics review*, *8*(1), 185-198.
- Sadekin, M. S., & Shaikh, M. A. H. (2016). Effect of e-banking on banking sector of Bangladesh. *International journal of economics, finance and management sciences*, *4*(3), 93-97.
- Sadekin, M., & Shaikh, M. (2015). Current status of e-banking practices in Bangladesh. *Scholar Journal of Business and Social Science*, *1*(1), 53-64.
- Tian, S., Yang, W., Le Grange, J. M., Wang, P., Huang, W., & Ye, Z. (2019). Smart healthcare: making medical care more intelligent. *Global Health Journal*, *3*(3), 62-65.

[i]https://archive.dhakatribune.com/bangladesh/2021/06/30/bangladesh-moves-25-spots-up-in-global-cybersecurity-index

[ii]Source:https://www.statista.com/statistics/976313/global-iot-market-size/ [2021]