Cyber Security: A way to take Artificial Intelligence on next level

Rokeya Khatun Shorna[a], Toufiqur Rahman Tonmoy[b]

rokeya15-9206@diu.edu.bd, toufiqur15-9039@diu.edu.bd
[a]*Daffodil International University, Dhaka-1212, Bangladesh*
[b]*Daffodil International University, Dhaka-1212, Bangladesh*

Abstract

Artificial Intelligence is bringing a revolution in the technological area. In this competitive era of technology, artificial intelligence is a blessing. In all stages of the technological areas everyone is using the applications of Artificial Intelligence (AI) and significant thing is this is making our life easier and more comfortable. Cybersecurity area is a challenging area while using the internet or making the internet a huge part of life. In this competitive era, in every step, we need to use the internet. This is making our life small and easy. But we know where there is an advantage, there must have some risk. And the threat in this area is huge where we need the help of cybersecurity. The sectors of cyber threats are many. In every step of using the internet, we face threats. Need to mitigate all the threats. That's why we are developing this picture. This is a huge sector and it is not possible to work with all sectors. In this research, we attempted to discover some reasons for cybersecurity as well as potential solutions. We applied Artificial Intelligence (AI) to uncover cyber threat solutions that will aid in the development of the entire system.

Keywords: Artificial Intelligence; Technology; Cybersecurity; Challenge; Cyberthreats.

1. Introduction

The main aim of this paper is to create awareness for the Cyber security by taking Artificial Intelligence (AI) on the next level. The use of technology, methods, and policies to safeguard systems, networks, programs, devices, and data from cyber-attacks is known as cyber security. The goal of cyber security is to limit the danger of assaults and defend against illegal technology absorption. Cyber security works for the benefits of the protection of networks and data from unauthorized accesses, improve the system of information security and business continuity management, building on the company credentials with the correct security controls and many more purposes. There are many kinds of cyber security attacks, Include as Malware which encompasses various kinds of attacks like viruses, worms, spyware etc. Password attacks, Cross-site scripting, Phishing are some other kinds of cyber security attacks. The main point of cyber security is to focus on keeping software and devices free from the unwanted threats. The term "cyber security" refers to a collection of methods and technologies designed to prevent unauthorized access, attack, change, or destruction of networks, computers, data, and applications [7]. Social engineering assaults are costly,

according to a global study of 853 IT experts performed in the United States, United Kingdom, Canada, Australia, New Zealand, and Germany in 2011 [13]. According to a study conducted by the Engineering Employers Federation (EEF) in 2018, of the 48 percent of manufacturers who claim to have been impacted by cyber-attacks, about half have experienced financial or other company losses [8]. From 2017 to 2021, global cybersecurity spending is predicted to exceed $1 trillion, with spending on cybersecurity already up nearly 40% from 2013 to $66 billion [9]. In the last few years, cybersecurity research has begun to look into Artificial Intelligence as a means of preventing cybercrime. We sought to concentrate on how Artificial Intelligence (AI)-based cybersecurity injection could improve the detection of intruders. Artificial Intelligence (AI) systems can be trained to generate alerts for dangers, new types of malware, and the protection of important data for businesses. For the recent year 2021, the industries agree that they will find an endless list of Artificial Intelligence security platform in the marketplace to protect their required data and information. As this technology is automated decision-making and evaluation processes dispense a huge range of protection from malicious activity than legacy solutions. Point that AI can be more protective and detector devices for unwanted and suspicious activity. According to the new research from ISACA study of Cybersecurity in May 2021, it operates that more than 3600 cybersecurity leaders reports consistent challenges to find qualified, skilled candidates and teams stay strongly correlated to an upgrowing types of cyberattacks. According to Cybersecurity Ventures, there will be 3.5 million cybersecurity employment vacancies by 2021, up from 1 million last year [16]. Another key advance in the AI area since the 1980s has been the rise of machine learning technologies, which aid computer systems in learning and adapting to diverse environments by leveraging their prior experiences, patterns, and knowledge [21]. Proper protection with Artificial Intelligence technology is extremely important; otherwise, around 3.5 million roles in Cybersecurity will be required in the coming year, costing a total of $3 trillion globally. We have discussed on top 10 Cybersecurity threats in 2021 on this paper.

The contributions of this research are given below:

- Tried to present an overview of the uses of Artificial Intelligence (AI) which is to identify cyber threats.
- Discussed the possible malicious activities detection by the help of modern AI.
- Consulted about trained Artificial Intelligence (AI) for decreasing the cyber risk and able to use cyber network safely.

Artificial Intelligence currently helps firms cut operating expenses, increase efficiency, and provide the best possible customer experience [20]. This modern technology can be helpful to centralized the database for the business information and client services.

The following is how the rest of the paper is organized: Section 2 states the related works in this field where used Artificial Intelligence (AI) to protect the cyber system. The cybersecurity challenges and solutions of them are analyzed in section 3. Section 4 elaborates Artificial Intelligence (AI) techniques for cybersecurity. Finally we conclude this paper and shows future perspective in section 5.

2. Related Work

Paul J. Schmick, Conteh, Nabie Y., et al. Evaluated the vulnerabilities of an organization's information technology infrastructure by this study [1]. Lee, Hadlington, et al. Dedicated to the investigation and classification of dangers posed by malicious attacks by current workers who are unhappy with the company or motivated by financial gain [2]. David, Rios Insua, et al. Proposed the frameworks, serving as template for more complex problem of cybersecurity by the risk analyzation [3]. Fernando, Alves, et al. Worked on a Twitter-based streaming threat monitor, which delivers a continually updated summary of the cybersecurity threat landscape affecting a monitored system [4]. Maria Pinto-Albuquerque, Gasiba, Tiago Espinha, Ulrike

Lechner, et al. Developed the awareness of cybersecurity challenges for software developer to produce the secure code [5]. Iqbal H., Sarker, et al. Worked on Massive shifts in technology and its operations in recent days, and data science is driving the change is being undergone by cybersecurity [6]. Said A., Salloum, et al. Reviewed of network analyzation for cybersecurity on machine learning and deep learning techniques [7]. Marianna Lezzi, Corallo, Angelo, Mariangela Lazoi, et al. Profound the branches affect business performance of increasing number of cybersecurity and also explained the impacts of cyber-attacks in critical industrial equipment [8]. Sherali, Zeadally, et al. By assessing both its strengths and drawbacks, researchers looked into the potential of artificial intelligence in developing cybersecurity solutions [9]. Zeinab, El-Rewini, et al. Sensing, communication, and control are three layers of the system proposed to better understand vehicle security concerns [10]. Deval, Bhamare, et al. Looked forward at the shift of the Cybersecurity for Industrial Control Systems from stand-alone systems to cloud-based environments [11]. Kathleen M., Carley, et al. Defined emerging area, research issues and types of tools needed on social cybersecurity [12]. Hongsong Zhu., Wang, Zuoguang, Limin Sun, et al. The original meaning of social engineering in cybersecurity is examined in the context of conceptual problems [13]. Tim Finin, Satyapanich, Taneeya, Francis Ferraro, et al. Conducted experiments on Cybersecurity event information which detected by the text subsystem [14]. Mostafa, Mohammadpourfard, et al. Evaluated the system using load data from the operator with different attack scenarios [15]. Kirk, Bresniker, et al. Provided recommendations to cyber analysts and help to detect the threats by the help of Artificial Intelligence (AI) and machine learning (ML) [16]. Alberto Perez, Veiga, et al. Introduced the need for cyber security tactics to evolve and how Artificial Intelligence (AI) may be used to help solve some of the difficulties, as well as an outline of AI Network Security techniques [17]. Benoit, Morel, et al. Argued that cybersecurity calls for new and specific AI techniques developed with that kind of application in mind [18]. Lazaros Iliadis, Demertzis, Konstantinos, et al. Presented a Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security [19]. Narcisa Roxana, Mosteanu, et al. The benefits of employing Artificial Intelligence addressed awareness in order to overcome fear in exploring new technologies because of cyber-attacks [20]. Sherali, Zeadally, et al. Identified both strengths and weaknesses by AI's potential in improving cybersecurity solutions [21]. Praveen Kumar, Donepudi, et al. Planned to reveal insight into the idea of artificial intelligence and its fields to upgrade and improve cybersecurity [22]. Ajay, Nagarajan, et al. Taught everyday users the requisite cybersecurity skills through gaming, beyond the current state of practice [23]. Ivan Zelinka, Truong, Thanh Cong, Quoc Bao Diep, et al. The goal of this presentation is to give an overview of how artificial intelligence can be used in both offensive and defense in the context of cybersecurity [24]. Michael C., Horowitz, et al. Examined the potential consequences of advances in artificial intelligence for the national security community [25].

3. Cybersecurity Challenges and Solutions

We have discussed on top 10 cyber threats and challenges in 2021 with the cyber solutions here-

3.1.1 Phishing Attacks

In this attack, the attacker will pretend to be someone trustworthy, like as our authority where we work or the bank policy where there is our full faith. Usually the attacker emails from an intimate way, but slightly altered email address. There can be a link or attachment in that email. Then request access to a website with information such as your social security number or bank account number. In 2019, phishing was responsible for 32% of confirmed data breaches and 78% of all cybercrimes. Cybercriminals were able to construct phishing schemes utilizing cloud applications in 2021.

3.1.2 Cloud Jacking

Now a days a new threat arrived in cyber security world. Cloud jacking, where a computer network can be affected by others user. And most alarming thing is this theft is being executed from social engineering process. So, it is being hard day to day to detect these types of attack. In this type of threat other user can stole your data from your device and also ransom ware can be included in this. Now a days our world is being very much competitive. In this period, it is very much needed to cope with the world. Keep updated with people always. And for the reason there is clod computing. From a cloud computer network the computer or devices are attached to each other. So, accessing data is not so hard. But where are pros, there will be cons. In cloud network some hackers or spammers always trying to access in network, and once they could reach all data can be gone. From a stat 96% companies are in fear to lose their data from cloud computing. Also 70% companies already face cloud jacking and their data lose. India are on to much risk as their risk is 93%. From all the risk attack in computing cloud jacking risk possibility is 17%. This shows how much dangerous cloud jacking is. Cloud jacking can be caused by two ways. Misconfiguration and data theft. Data theft is an ethical issue but misconfiguration can be solved. From a stat in USA, 77% caused from misconfiguration where as 23% from data theft. Cloud jacking can be solved, just all we need to be aware of the issue.

3.1.3 Growth of Hacktivism

The combination of hacking and activism is the Hacktivism. The act of compromising digital devices and networks by gaining unauthorized access to an account or computer system is known as cyber hacking. Hacking is some kind of illegal activity and stealing data by the cyber criminals which favors the social and political agendas in a wrong way. Most of the time, the motive of the hackers to harm the visibility of the websites or the protocols. According to the IBM X-Force report in 2021, hacktivists manifest their interest in stealing the data of multinational and government corporations which was 25% of data stealing and leak attacks. It is one kind of denial of service attack (DoS) which shuts down any systems to protect user access.

3.1.4 Mobile Malware

Mobile malware is a kind of software which is designed to get access in private data from smart phones or private data. Hackers or spammers design this kind of software with such system, so that user will be attracted to click or use that software. When user clicks the access of private data gone to hackers. It is a great threat while using any network. But the good news is now a day companies are restricting and recruiting people to prevent their operating system from malwares. There are different kinds of mobile malware which can down the system or take over access on devices. The evolution of mobile malware is not so updated. It is running through years. In 2000 the first malware was founded named “The first virus”, In 2004, “The worm” was invented, which another name was Cabir. In 2007, “The first mobile spyware” was invented, and in 2011, “The evolution of Cabir” comes to the light. So, it can be seen that from very past mobile malware is creating panic in the era of mobile network. There are different types of mobile malwares. Such as:

- Remote access tools
- Trojans
- Ransomware
- Advertising click fraud

From years to years those are creating threats in mobile network. Also, there are some ways that’s how mobile device can be attacked with malware:

- Malicious application download
- Opening malicious emails
- Using non-secure Wi-Fi
- Mobile with risky operating systems

But the news of hope is now a there are ways to void mobile malware and also many researches is been running to sop this kind of threats. Also, people need to keep in mind that they also have to use devices with safety and securely.

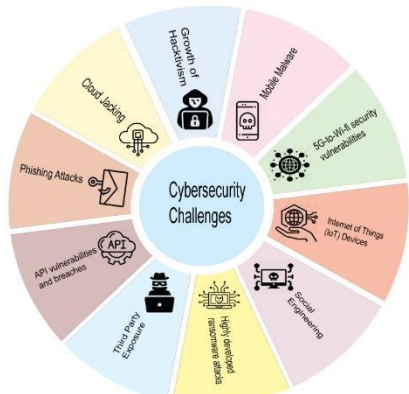


Figure: Cybersecurity Challenges

3.1.5 5G-to-Wi-fi Security Vulnerabilities

New generations has so many curiosities about 5G networks which will let them use their favorite devices more proficient. Along with that, the new generations are going to be the victim of cyber-attacks. Wi-fi security vulnerabilities which allow hackers to change the smart switches. From the 5G network to Wi-fi networks to save the flaws and bandwidth in the procedure will allow the hackers to compromise security system. Attackers find new vulnerability to access other's personal data and information throughout this.

3.1.6 Internet of Things (IoT) Devices

In the recent time, most of us are interested towards Internet of Things (IoT) devices because of their robust reaction time and the lower cost. They are popular for their processing of cloud technology too. With the rising of this technology, cybercrimes are also increasing day by day along with this. The IoT market has gained the potentiality of 418 billion USD and it is expected that it will gain around 1.567 trillion USD within 2025. Hackers are destroying the channel nodes by promoting prosperity plus the lawable sales traffic for the community. Sometimes for this method, the cybersecurity protocols are may vulnerable.

3.1.7 Social Engineering

The trick and strategies of the hackers for manipulating users to give up their secret information is the social engineering. Hackers use this social engineering methods because of its easy way to utilize our trust and after that they find out the ways to hack the user's software. Most of the social engineering attacks happen by the official emails which look genuine.

3.1.8 Highly Developed Ransomware Attacks

A ransomware attack is a kind of malware. Cybercriminals usually uses it to get access to others data. It very much dangerous malicious virus which can block access of user and stole data permanently. Cyber

criminals invented it to get full access of any network. The history of ransomware attack is huge. From 2000s ransomware is creating threats upon cybersecurity. The first ever ransomware attack was on 1989. The attack caused a huge loss. Almost 20k floppy disk was stole. So, it can be easily imagined that how much dangerous a ransomware can be. Most popular ransomware is two types. Such as:

- Locker Ransomware: In this kind of ransomware user can deny the request of cybercriminal. But the request is not fully over. This can disable the access of mouse and keyboard. Locker ransom doesn't set target for important files. It only wants to stop the system.
- Crypto Ransomware: This type of attack encrypts data. All documents, pictures can be observed from other users. Often the main user remains in panic, because his/her all activity is exposed it to the others. So basically, in this case there is no privacy.

So, the effect of ransomware can be more than dangerous and this can give a user mental and physical pressure too.

3.1.9 Third Party Exposure

Employee and customer data, financial information and operations are somehow depending on the vendors for a variety of services. This partnership may cause the risk of the internal hacking processed. This partnership has a business value, because of that it can't be avoidable. To understand and gain knowledge about the potentiality is the beginning step of third-party exposure.

3.2.0 API Vulnerabilities and Breaches

When any Uniform Resource Identifier (URI) attached to the request over the internet, hackers share the vulnerabilities of any other resource accessible way on the internet. This is the way how APIs vulnerabilities happen. Data branches can be physical, electronic and skimming. They all are unique but they share the same amount of risk. We may not take this API security seriously but API data breaches can be happened throughout the third-party exposure.

Solutions:

- Train the staff
- Network Perimeter and Endpoint Security
- Keeping the software and systems fully up to date
- Controlling the access system
- Wi-fi Security
- Detecting new Threats
- Battling Bots

4. Artificial Intelligence (AI) Techniques for Cyber security

Artificial Intelligence (AI) prescribes the technology that can act on their own, understand, learn, take decision and derived the information. In this modern time, Artificial Intelligence (AI) works in some techniques:

1.1 *Assisted, Augmented and Autonomous Intelligence*

Assisted Intelligence is widely available in this recent time, it works to improve the system which people and organizations are doing already. Develop the previous system. People and organizations can now do things they couldn't do before thanks to augmented intelligence. Autonomous Intelligence is a futuristic technology that involves machines that behave independently.

1.2 Neural Networks

It is inspired by the functions and working of the human brain. It is a series of algorithms that effort to accept the connections in a set of data with a process that mimics the human brain conducts. Usually neural networks prescribe to the system of neurons. It uses a biologically-inspired programming paradigm which will be able to observe the data and learn it throughout the computer system. Algorithm works as nodes and weight-wise, each node sets a weight to its input description how right or wrong. The addition of the weights is the final output.

1.3 Expert System

It works by mimicking the thinking of human experts. It is a computer system that imitate the decision-making ability of a human. The knowledge-based system and inference engine are the two sub-system of this knowledge base system which is the best example of expert system.

1.4 Deep learning

It is a type of machine learning and artificial intelligence (AI) which mimics the mode of humans gain a particular type of knowledge. To collect, analyze and interrupt a large number of data can be processed within faster and easier way by the deep learning. In the recent time, image recognition through deep learning even better than human activities. With the different kinds of algorithms, it is being extreme beneficial.

1.5 Machine Learning

It has the ability to learn by statistical techniques. Basically, it learns experience. Machine learning give its working ability more when it works for any specific work rather than a large number of works. The three types of machine learning algorithms are supervised learning, unsupervised learning, and reinforcement learning.

The advantages with these Artificial Intelligence (AI) techniques are-

Techniques	**Advantages**
Assisted, Augmented and Autonomous Intelligence	Widely available
	Proactive
	Protection against DDoS
	Features that act on their own
	Reactive

	Update from previous work
	Mobility
	Emerging understand
Neural Networks	Detect DoS
	Well range of operation speed
	Forensic Investigation
	Detect Intrusion
	Use biologically-inspired programming paradigm
	Prevent the System
Expert System	Domain specialized
	Mimic and think of human expert
	Knowledgeable
	Decision Support
	Detect intrusion
Deep learning	Learn data representation
	Highly capable to recognize
	Able to do task along with the algorithms
Machine Learning	Statistical techniques to learn
	Work for a specific work

Table: Advantages of AI techniques.

5. Conclusion and Future work

Artificial Intelligence (AI) can be beneficial for cybersecurity in various way. In this research we have tried to utilize the cyber security through AI. Cybersecurity is one of the alarming topics nowadays. If anyone tries to cope with the online world he must have to face some security challenges. And also, around people always some crimes are happening for the lacking of cybersecurity. In this paper, we tried to find out some problems without cybersecurity. How much it can be dangerous and how much harmful all were discussed. In today's world, each and every time the security is been broken. All the threats of the online or cyber world we discussed can be increased. So, all the steps we mentioned are not enough. In the future world, to cope up there will be more ways. We Know for surviving, people invented the survival types of equipment. It can be expected that more and more technologies are yet to come for doing a revolution in this era. The news of hope that Artificial Intelligence is a blessing in the Technology Sector. And cybersecurity sector is also included in it. More technologies are coming through artificial intelligence. Now the brain of humans is more aware. As a result, AI is contributing its effectiveness in this sector. In future, we can hope that one-day cyber security would be the greatest innovation in cybersecurity sector.

Acknowledgements

These and the Reference headings are in bold but have no numbers. Text below continues as normal.

References

Conteh, Nabie Y., and Paul J. Schmick. "Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks." Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention. IGI Global, 2021. 19-31.

Hadlington, Lee. "The “human factor” in cybersecurity: Exploring the accidental insider." Research Anthology on Artificial Intelligence Applications in Security. IGI Global, 2021. 1960-1977.

Rios Insua, David, et al. "An adversarial risk analysis framework for cybersecurity." Risk Analysis 41.1 (2021): 16-36.

Alves, Fernando, et al. "Processing tweets for cybersecurity threat awareness." Information Systems 95 (2021): 101586.

Gasiba, Tiago Espinha, Ulrike Lechner, and Maria Pinto-Albuquerque. "CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments." arXiv preprint arXiv:2102.05345 (2021).

Sarker, Iqbal H., et al. "Cybersecurity data science: an overview from machine learning perspective." Journal of Big data 7.1 (2020): 1-29.

Salloum, Said A., et al. "Machine Learning and Deep Learning Techniques for Cybersecurity: A Review." AICV. 2020.

Corallo, Angelo, Mariangela Lazoi, and Marianna Lezzi. "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts." Computers in industry 114 (2020): 103165.

Zeadally, Sherali, et al. "Harnessing artificial intelligence capabilities to improve cybersecurity." Ieee Access 8 (2020): 23817-23837.

El-Rewini, Zeinab, et al. "Cybersecurity challenges in vehicular communications." Vehicular Communications 23 (2020): 100214.

Bhamare, Deval, et al. "Cybersecurity for industrial control systems: A survey." computers & security 89 (2020): 101677.

Carley, Kathleen M. "Social cybersecurity: an emerging science." Computational and mathematical organization theory 26.4 (2020): 365-381.

Wang, Zuoguang, Limin Sun, and Hongsong Zhu. "Defining social engineering in cybersecurity." IEEE Access 8 (2020): 85094-85115.

Satyapanich, Taneeya, Francis Ferraro, and Tim Finin. "Casie: Extracting cybersecurity event information from text." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34. No. 05. 2020.

Mohammadpourfard, Mostafa, et al. "Ensuring cybersecurity of smart grid against data integrity attacks under concept drift." International Journal of Electrical Power & Energy Systems 119 (2020): 105947.

Bresniker, Kirk, et al. "Grand challenge: Applying artificial intelligence and machine learning to cybersecurity." Computer 52.12 (2019): 45-52.

Veiga, Alberto Perez. "Applications of artificial intelligence to network security." arXiv preprint arXiv:1803.09992 (2018).

Morel, Benoit. "Artificial intelligence and the future of cybersecurity." Proceedings of the 4th ACM workshop on Security and artificial intelligence. 2011.

Demertzis, Konstantinos, and Lazaros Iliadis. "A bio-inspired hybrid artificial intelligence framework for cyber security." Computation, cryptography, and network security. Springer, Cham, 2015.

161-193.

Mosteanu, Narcisa Roxana. "Artificial Intelligence And Cyber Security–Face To Face With Cyber Attack–A Maltese Case Of Risk Management Approach." Ecoforum Journal 9.2 (2020).

Zeadally, Sherali, et al. "Harnessing artificial intelligence capabilities to improve cybersecurity." Ieee Access 8 (2020): 23817-23837.

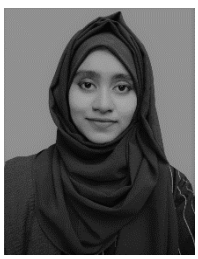
Donepudi, Praveen Kumar. "Crossing point of Artificial Intelligence in cybersecurity." American journal of trade and policy 2.3 (2015): 121-128.

Nagarajan, Ajay, et al. "Exploring game design for cybersecurity training." 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER). IEEE, 2012.

Truong, Thanh Cong, Quoc Bao Diep, and Ivan Zelinka. "Artificial intelligence in the cyber domain: Offense and defense." Symmetry 12.3 (2020): 410.

Horowitz, Michael C., et al. Artificial intelligence and international security. Center for a New American Security., 2018.

.



Rokeya Khatun Shorna is born in Pabna, Bangladesh on 2nd November, 1997. Recently completed her B.S.c in Computer Science and Engineering (CSE) from Daffodil International University (DIU) in Dhaka, Bangladesh. She is going to start her M.Sc degree and wants to complete her higher studies in the top ranked University. She has worked on some well-known books as a writing contributor. The book titled: “Art of living” (published in DIU, 2019). She worked in some organizations too for the underprivileged children. In this recent year, her another research paper got accepted which was “Development of Multiple Regression Model for Rainfall Prediction” in CIS Conference. Ms. Rokeya wants to give her major focus on the research theme of “Artificial Intelligence (AI)”. From her University period, she is a member of IEEE DIU student branch and IEEE Computer Society Bangladesh chapter. Now she is looking forward to work more on Artificial Intelligence (AI) sector.



Toufiqur Rahman Tonmoy, is born in Rajshahi, Bangladesh on 3rd March, 1998. Recently he has completed his Graduation in Computer Science and Engineering (CSE) from Daffodil International University in Dhaka, Bangladesh. He is going to start her M.Sc degree and wants to complete his higher studies in the top ranked University. He has worked on some well-known books as a writing contributor. The book titled: “Art of living” (published in DIU, 2019). He is working in some organizations too for the underprivileged children. He has a huge interest in research on various things and wants to enhance his knowledge by researching and exploring things.