Cyber Crime Trend in Bangladesh, an Analysis and Ways Out to Combat the Threat

Shusmoy Kundu[1,2], Khandaker Annatoma Islam[1,3], Tania Tahmina Jui[1,4], Suzzana Rafi[1,5], Md. Afzal Hossain[1,6], Ishraq Haider Chowdhury[1,7]
[1]Department of Computer Science and Engineering,
Military Institute of Science and Technology, Dhaka-1216, Bangladesh.
[2]kshusmoy14@gmail, [3]annatomaislam.mist14@gmail.com, [4]taniajui226@gmail.com,
[5]suzzanarafi@gmail.com, [6]ayonarnab@yahoo.com, [7]ishraq.h.c@gmail.com

***Abstract*—In this paper an analysis has been carried out on the cyber attacks, that have happened in the recent years. Based on the analysis the cyber attack trend in the financial sector of Bangladesh has been investigated. The study is further extended to identify the causes of cyber heist in the financial sectors. The existing legal framework of Bangladesh for dealing with the cyber crimes has also been investigated in this paper. The analysis results are presented in appropriate graphs and charts. Finally a few recommendations are put forward for combating the increasing cyber crimes in the world, and in Bangladesh in particular.**

***Keywords*—Cyber security, cyber crimes, SCADA, code of ethics, legal issues.**

I. Introduction

Cyber Security is a security system to protect the computing devices and computer network where the important data are stored, retrieved and interchanged against any kind of attack or intersection. Cyber security includes application security, information security, network security, disaster recovery or planning, operational security and so on. All over the world all most all the organizations and enterprises are using computers, cloud and many others server and devices. All the data which belong to that companies are saved in the data base. They are supposed to be seen only by the employees and other members who are related to that organization. Sometimes they have to send their secret data from one place to another over the internet. Here professionals are engaged in the art of secret communication; i.e., have developed mechanisms for ensuring confidential information is not leaked to unauthorized parties. The more people are trying to access any program or system in an unauthorized way, the more information and data need to be saved in a secured and protected way.

Cyber crime is a bi-product of the ever-increasing development in the areas of information and communication technology (ICT). The attackers mainly attack the confidential data of the organizations or personal information thereof. The most targeted organizations are hospitals, government offices, police stations, financial institutions, Research and Development (R&D) organizations and other telecommunication firms etc. In this paper we shall analytically examine the cyber security scenario in the world with an in-depth emphasis in Bangladesh. Thereafter, we shall discuss the cyber security trend in the financial sector of Bangladesh. After that we shall put an endeavour to find the ways out to combat cyber crime in Bangladesh.

We organize the rest of the paper as follows. Background study of our work is discussed in Section II. In Section III, we are going to discuss about the major cyber attacks in recent times. In Section IV a comparison is given of cyber attacks among some other countries. Investments in cyber security measures by government and ICT organizations will be highlighted in the Section V. The trend of cyber attacks in Bangladesh are discussed in the Section VI. Next Section VII is about the legal framework to combat cyber crime in Bangladesh. The following Section VIII contains the ways out to combat cyber crimes and finally Section IX concludes the paper.

II. Literature Review

Shang, Jiang, Li and Wang [1] tried to combine the available clustered knowledge on cyber security into one big knowledge base and use that to train an entity recognizer. Thus the entity recognizer will be able to gain knowledge from integrated knowledge base and be able to identify any cyber security related entity from text.

Duić, Cvrtila and Ivanjko [2] worked with a goal to find more effective and long lasting ways to combat cyber attacks and crimes happening frequently around us in the world. They emphasized on how these cyber attacks are going to be threat to international relations and what is the way out to fight this using NATO's planning process for protection from cyber crimes.

Roldán-Molina, Almache-Cueva, Silva-Rabadão, Yevseyeva and Basto-Fernandes [3] presented their work to help in estimating the probability of cyber security risks and to form cyber security strategies by building a software.

Azad, Mazid and Sharmin [4] presented their work wherein they have highlighted the cyber crime laws of Bangladesh.

Teoh and Mahmood [5] discussed about the relationship between the development of cyber security strategy and the successful growth of economy.

III. Cyber Crime in Global Scenario

A. WannaCry Ransomware

On 12 May, 2017, the ransomware WannaCry has begun to spread. It has been reported that, within a day it infected more than 230,000 computers in over 150 countries. Parts of the United Kingdom's National Health Service (NHS), Spain's Telefonica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide. The WannaCry ransomware targeted computers running the Microsoft Windows operating system by encrypting data and files and then demanded ransom payments in the Bitcoin cryptocurrency. Viruses are normally spread as an attachment on an email or other downloaded file but WannaCry is a different type of ransomware because it can spread through a local network on its own. The ransomware has hit organizations using aging technology and outdated software [6]. For the remedy for this ransomware, a 22-year-old web security researcher from North Devon in England known as MalwareTech researched on this ransomware and analyzed the problem and code. Then he discovered an effective kill switch by registering a domain name he found in the code of the ransomware. Kill switch is a mechanism which remotely stopped any system or software without doing any harm and deleting any data. But cyber criminals are fighting back by modifying the code for further attack.

B. Petya Ransomware

Petya is a kind of ransomware which also encrypt the data and demand for ransom through bitcoin. Petya 1st is introduced in 2016. Till now there are two versions V1.0 and V2.0. It mainly infects the computer's Master Boot Record (MBR). When the malware is installed, it overwrites the Windows bootloader and then triggers a restart. It may come to the computers in many ways. But when user tries to install it, pretends as a normal software, then it shuts down the operating system and infects the boot loader. Then there will pop out a message which is similar with the message which user usually gets when repairing any system. But it shows the percentage of progress of file encrypting. After encryption, it will give a danger message which will tell to press any key, then it will pop out another message that user's data has been encrypted, for restoring the data the user has to pay the ransom though the bitcoin [7]. On 27 June, 2017, the Petya V2.0 has been started to spread. On that day, Kaspersky Lab reported infections in France, Germany, Italy, Poland, the United Kingdom, and the United States, but the majority of infections targeted Russia and Ukraine, where more than 80 companies initially were attacked, including the National Bank of Ukraine. Many organizations in Ukraine were affected, including government sectors, banks, state power utilities and Kiev's airport and metro system. For the solution, when the file is encrypting that time if process can be stopped, it can be saved from encryption. Many anti-virus companies claim that their software has been updated for preventing this type of encryption. Kaspersky also says its security software is now capable of spotting the malware [8]. It is safe to keep using all the updated software and anti-virus.

IV. Comparison of Cyber Attack among Other Countries

Almost all the countries over the world are under the cyber-attack threat. Due to lack of security any country's organization can be victim of the cyber-attack. A list of countries which are lowest malware infected [9] is shown in Figure 1.

A pie chart of countries with highest malware infection rates computers is shown below in Figure 2. The highest infected country is China and the lowest one is Poland [9].

Supervisory control and data acquisition (SCADA) is a system architecture of software or hardware for process control. It is a center control system. It consists of controller network interfaces input or output and gathers real time data. It uses peripheral devices like programmable logic controllers and discrete PIF controllers to the interface. The threat on SCADA is not new. In the network communication system an effective way of gaining the control means operating the system in real time. This communication can be attacked by the attacker. In September 2011, Russian hackers took gain

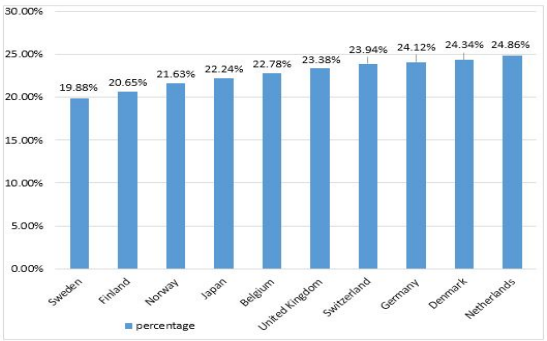

Fig. 1. The List of Countries with Lowest Malware Infection Rates in Computers.

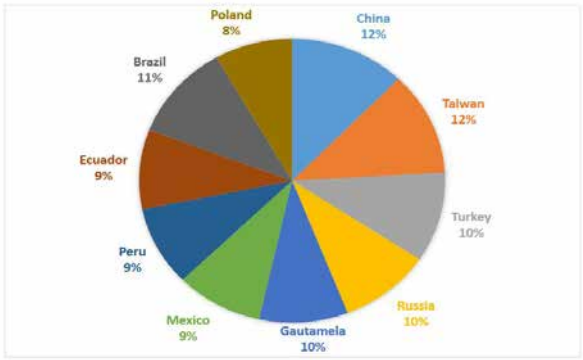

Fig. 2. The Pie Chart of Countries with Highest Malware Infection in Computer.

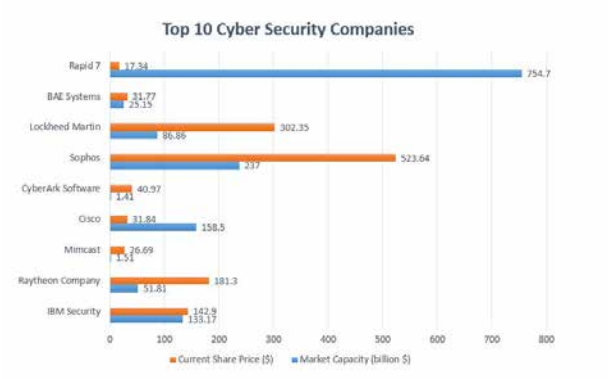

Fig. 3. Top 10 Cyber Security Companies around the World.

on the US SCADA, but it was not reveal until November 8^{th} [10]. GE SCADA can be attacked by the attackers. The use of network communication in these systems has proven to be an effective way of gaining a means for remotely operating and maintaining these infrastructures in real-time. Therefore, these have become vital assets providing a functionality otherwise impossible. However, this also opens up the way for new threat vectors that can potentially compromise the efficient and secure operation of these systems.

The Table I below exhibits sector wise cyber attacks in various countries during the period 2012 to 2017, [11].

V. Investments in Cyber Security Measures by Government and Private ICT Organizations

Cyber Security market, with its growing demand now-a-days remains in the most expanding one in comparison to other fields. With the technological advancement we are losing our privacy and confidentiality also. To cope up with the situation companies have to invest more and more to protect their valuable information and data being hacked. The world wide cyber security market is going to touch the $1 trillion boundary in a span of 5 years 2017 to 2021 [12]. Below we can see a chart (shown in Figure 3) that is gathered by the Investing News Network (INN) showing market capacity and current share price of popular cyber security companies [13].

TABLE I
Sector wise cyber attacks in various country

Organization	Sectors	Year
Indian Banks data breach	Financial	2017
JPMorgan Chase data breach	Financial	2014
VISA and Master Card	Financial	2012
Bangladesh Bank Government	Financial	2016
United Kingdom National health service	Medical	2017
National Bank of Ukraine	Govt. Financial	2017

Here according to Investopedia, "Market capitalization refers the total dollar market value of a company's outstanding shares [14]. Commonly referred to as 'market cap', it is calculated by multiplying a company's shares outstanding by the current market price of one share."

Reference [15] represents investments of various companies is shown in a bar chart in Figure 4.

Here in the chart we can see that The White House will invest more on cyber security as a part of President's Fiscal Year 2017 budget. They has done it for their nations future security. Microsoft will be spending same in this field. The J.P. Morgan Chase & Co. has doubled their cyber security investment budget.

In Bangladesh the situation is a bit frustrating. There is hardly any ICT organizations in private sector who allocate and spend mention able amount for ensuring their net security. However in the government sector the situation is emerging day by day. The IT sections of various government organizations are now allocating budget for enhancing security of their websites and network. Good news is that ICT division (*www.ictd.gov.bd*) have undertaken a mega project for developing cyber security labs in various universities and organizations of

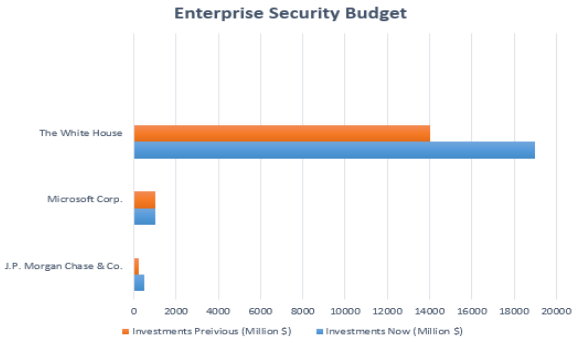

Fig. 4. Enterprise Security Budget.

the country [16].

VI. Cyber Attack Trend in Bangladesh

Bangladesh is a developing country. In most of the countries like Bangladesh have limitations in information accessing and it is because of having very less knowledge about the existing infrastructure. Cyber crime is a property related crime. Victims are not the priority here, only snatching of properties such as information, data etc. is the purpose of this crime. In our country most of the banks are at high security risk. According to Bangladesh Institute of Bank Management (BIBM), approximately Tk 1,793 crore was invested in the banking IT sector in 2016. Still this banking sector is not cyber crime free at all. A study of Bangladesh Institute of Bank Management (BIBM) says that, a total of 52% of the banks in our country are at high risk of cyber security issues (shown in Figure 5). Out of that 52% banks, 16% banks are at very high risk and 36% banks are high risk [17]. Risks in 32% banks are moderate, 12% banks are at low risk and the remaining 4% of banks are at very low risk region. Cyber security in the banking sectors is a burning question in recent times especially after the Bangladesh Bank Heist.

The incident Bangladesh Bank Heist held on 4^{th} February 2016, where the hackers (still unknown) tried to steal $1 billion. The hackers managed to get $81 million sent to Rizal Commercial Banking Corporation in the Philippines and PABC bank in the Srilanka via four different transfer requests and an additional $20 million sent to Pan Asia Banking in a single request. The malware's name was evtdiag.exe. The attackers are called Reuters [18]. The hacker did this through a malware which worked on swift messaging system. This malware deletes any incoming message and the confirmation message before sending the office printer [7]. On 4^{th} February, Thursday after working hour, the malware was activated. As Friday was holiday in Bangladesh, there was no one for monitoring the transition message. The attacker gave many request for transition, not all succeeded. They kept trying to transition, after that they were able to transfer money though their fake accounts. After that when on Sunday the bank is opened after weekend, the officials noticed that something wrong had happened because the malware also stopped printer from printing the transition information. The malware also handled the log in and log out process and also controlled the server and modification. Then they said to Philippines bank to stop the transition, but that time in Philippines it was there weekend. The malware was programmed for activation up to 6^{th} February. After identifying the attack, the transition has been stopped, but the attacker succeeded to transfer $81 million.

Credit cards, debit cards etc are denoted as "plastic money" are the replacement of conventional financial components paper money in the current living time. The use of ATM is convenient but has a negative phase, which comes out in the form of "ATM frauds". "Internet fraud" is the use of internet services or software with internet access to defraud victims or to otherwise take advantage of them using various components of the internet, like chat rooms, email, forums, or websites - to execute fraudulent transactions. Bank criminals are making utilization of different electronic medium, for example, web, email, and encoded messages for their fraudulent activities [19].

In the last few years, several security breaches had happened in the banking sector of Bangladesh [19], some of those are shown in Table II.

VII. Legal Framework to Combat Cyber Crime in Bangladesh

The term Cyber Law is used to describe the legal issues related to use of information and communications technologies(ICT). An effective cyber law can play a vital role in ensuring that the cyber criminals are fairly and successfully tried and judged for their crimes. Cyber law is much needed to control the misuse and abuse of computer technologies in order to protect nations

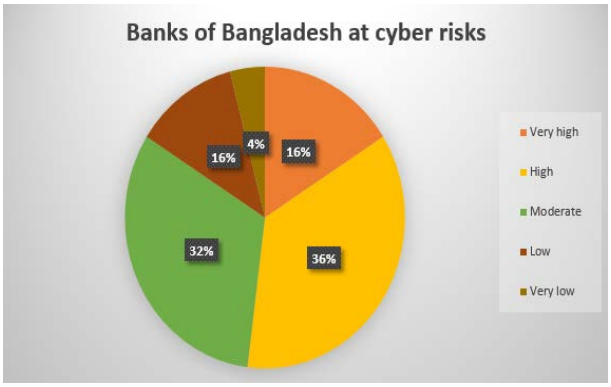

Fig. 5. Banks of Bangladesh at Cyber Risks.

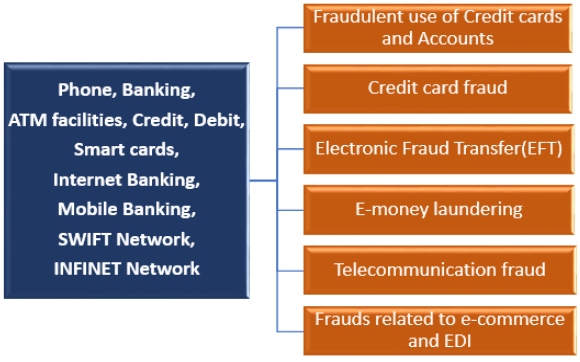

Fig. 6. Technology and related crimes.

TABLE II
SECURITY BREACHES IN BANGLADESH

Time of Occurrence	Incident
January 06, 2013	Islami Bank Bangladesh site was hacked by Human Mind Cracker
2015	Accounts of a private bank were hacked and money was withdrawn
December 02, 2015	Sonali Bank's network security was broken and control was taken by the hacker for several hours
February, 2016	Attacks in six ATM booths of three commercial banks
February, 2016	Hackers stole $101 million from Bangladesh Bank

against cyber attacks and bring the perpetrators behind the bar. Most of the developed countries are already equipped with cyber security strategies and laws. Some of them are- Cyber security strategy in Singapore (2016), Finland's cyber security strategy [20], National Strategy for the Protection of the Switzerland against Cyber Risks [21] etc.

The legal framework to deal with cyber crimes in Bangladesh are given below:

Laws related to cyber security were first enacted in Bangladesh in 2006. [22] Section 57 of the ICT Act 2006 is related to cyber security. It says, "If any person, willingly publishes or broadcasts any material on website or any other electronic form that is false and vulgar, or given the situation upon reading, writing or listening to that material, any person can become derailed or dishonest, or which causes defamation, worsen or create the possibility to worsen the law and order situation, damage a person's or state's image, or harm or may harm religious feelings, or provocation is instigated upon any person or organization through these materials, then his/her such act will be a crime".

In the latest amendment(2013), offences under Section 57 were made non-bailable and the maximum penalty was extended to 14-year imprisonment.

- This section has aroused huge criticism amongst the citizens as it contradicts with freedom of speech and expression (constitutional right). As such the government is going to abolish this Section 57 by enacting a new law named 'Digital Security Act, 2016', which has been prepared by ICT division. [20]
- 'The National ICT Policy 2009' is a framework that tells us how to use ICT for the social and economic development of the country [23]. It includes creation of ICT infrastructure, research and development of ICT, application of ICT on various sectors etc.
- The Bangladesh government had approved this very effective Anti pornography act in 2012 [21]. It is believed to be Bangladesh's first law specifically controlling the spread of pornography. The law bans production, preservation, transportation and marketing of any kind of pornographic materials. Upon breaking the law, the criminal is given proper punishment.

VIII. WAYS OUT TO COMBAT CYBER CRIME

In order to combat cyber threats wholistic approach by both government and private organizations needs to be undertaken. Our government, through ICT division has already taken some measures in this regard. Yet it is not enough. Hackers or intruders find some way to hamper our privacy, mess with our valuable information and sometimes make damages that takes years to get over for a country like us. Here we shall propose measures that the concerned organizations may consider to deal with cyber security.

A. Investments in Cyber Security Aspects

Observing the cyber crime trend in Bangladesh it is needless to mention that both private and public sector need to invest substantial amount of their budget for enhancing cyber security measures. Bangladesh government has invested 40 crore BDT to build up cyber security branch in the ICT division [24]. At the same time private sectors are need to be encouraged to invest in cyber security aspects of their business.

B. Legal Framework

Our government has passed various legal acts to fight back the cyber attack and also stop digital harassment. We have ICT acts 2006, 2009, 2013(amendment), Draft Digital Act 2016 [25], [26]. The Draft Digital Act 2016 may be enacted at the earliest All these acts combine the cyber security in our country.

C. Seminar and Training

The government arranges various seminars, workshops at college, university and institution level to make people aware about the cyber crime issues. These seminars or workshops enlighten people about cyber crime happening around the world and also in our country and how to fight back them. In supervision of bdCERT many training programs are held [27].

D. CERT Group Formation

CERT means Computer Emergency Response Team. This team's responsibility is to deal any instant devastating situation arisen due to cyber attack. Bangladesh government has given us a 24*7 hours CERT assistance named bdCERT [27]. Each organization and institution need to form their individual CERT.

E. Cyber Security Strategy

Each and every organizations must have a strategy to combat cyber crime and take immediate decisions when needed. This strategy should be made as per the National Cyber Security Strategy [28].

F. Code of Ethics

Each organizations should have a culture of complying with code of ethics (ACM code) by their employees [29]. ICT education in universities and institutions need to include courses on engineering code of ethics in their curriculum. Bangladesh government has already made ICT education compulsory in its secondary and higher secondary level. In this curriculum code of computer ethics (ACM) may be incorporated.

IX. Conclusion

The current cyber attack trend in Bangladesh demands prompt attention for creating and maintaining robust and workable cyber security strategy to keep our cyber space safe and secure against any potential cyber attack. It needs to consider our country's economic capacity, availability of skills and resources. Government has prioritized this and invested a lot in ICT sector. But a strong cyber security strategy is yet to be prepared and put in action in our country. Comparison of cyber threats among various countries is shown in this paper. It also highlights the trend and statistics of cyber threats in various sectors like industry, finance and government. To combat the cyber crimes, the measures taken in foreign countries, as well as in Bangladesh are discussed here. Government and private sectors contribute in creating awareness for combating cyber crimes through holding seminars, conferences, workshops, trainings etc. The need for a culture of complying with codes of engineering ethics to deal with cyber crimes has also been mentioned. A few proposals have been put forward in this paper to enhance the cyber security strength of Bangladesh.

References

[1] H. Shang, R. Jiang, A. Li, and W. Wang, "A framework to construct knowledge base for cyber security," in *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, June 2017, pp. 242–248.

[2] I. Duić, V. Cvrtila, and T. Ivanjko, "International cyber security challenges," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2017, pp. 1309–1313.

[3] G. RoldÃąn-Molina, M. Almache-Cueva, C. Silva-RabadÃčo, I. Yevseyeva, and V. Basto-Fernandes, "A decision support system for corporations cybersecurity management," in *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, June 2017, pp. 1–6.

[4] K. N. M. Dr Mir Mohammad Azad and S. S. Sharmin, "Cyber crime problem areas, legal areas and the cyber crime law," July 2017.

[5] C. S. Teoh and A. K. Mahmood, "National cyber security strategies for digital economy," in *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, July 2017, pp. 1–6.

[6] "Wannacry cyber attack," https://www.thestreet.com/story/14147814/1/how-hackers-changed-their-style-in-the-wanna-cry-attacks.html.

[7] "Bangladesh Bank Attackers Used Custom Malware," https://www.pcworld.com/article/3060724/bangladesh-bank-attackers-used-custom-malware.

[8] "Petya virus new analysis," https://www.theverge.com/2017/6/28/15887496/petya-virus-not-actually-ransomware-analysis-shows.

[9] "Countries which are most vulnerable to cyber attacks," https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/, [Online; accessed 22-March-2017].

[10] "Scada," https://www.infosecurity-magazine.com/news/russian-hackers-behind-first-successful-us-scada/.

[11] "Bangladesh bank heist, swift software was compromised," https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-april-2017/.

[12] "Cyber security companies," https://cybersecurityventures.com/cybersecurity-500/, [Online; accessed 24-September-2017].

[13] "Cyber security market report," https://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-security-companies/, [Online; accessed 4-October-2017].

[14] "Market capitalization," http://www.investopedia.com/terms/m/marketcapitalization.asp, [Online; accessed 4-October-2017].

[15] "Cyber security market report," https://cybersecurityventures.com/cybersecurity-market-report/, [Online; accessed 24-September-2017].

[16] "Ict ministry news," http://doict.portal.gov.bd/site/page/73fa42ac-fae9-4c0b-bec7-5edbb6841e64/.

[17] "Dhaka tribune news," http://www.dhakatribune.com/business/banks/2017/05/05/banks-high-cyber-risks/.

[18] "Bangladesh bank heist, swift software was compromised," http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR.

[19] "Cyber crime scenario in bangladesh," http://www.icmab.org.bd/images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf.

[20] "Ict amendment 2013," http://www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat/.

[21] "Anti pornography act 2012," http://www.iiste.org/Journals/index.php/JLPG/article/viewFile/21714/21905http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct.

[22] "Ict act 2006," http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/97cc59c3_8f51_4d39_a84b_8c0b39ae3f62/ICT_ACT_2006.pdf.

[23] "National ict policy,2009," http://www.bcs.org.bd/img/upload/page/11.pdf.

[24] "Cyber security market report," https://www.ictd.gov.bd/project/proposed, [Online; accessed 4-October-2017].

[25] "Ict act 2006 bangladesh," http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?id=950&vol=37&search=2006/, [Online; accessed 25-September-2017].

[26] "Ict act 2009 bangladesh," http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?id=1011&vol=39&search=2009/, [Online; accessed 25-September-2017].

[27] "Cyber security market report," http://www.bdcert.org/, [Online; accessed 4-October-2017].

[28] "Cyber security market report," https://www.unodc.org/res/cld/lessons-learned/the_national_cybersecurity_strategy_of_bangladesh_html/The_National_Cybersecurity_Strategy_of_Bangladesh.pdf, [Online; accessed 4-October-2017].

[29] "Acm code of ethics," http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct/, [Online; accessed 27-September-2017].

Shusmoy Kundu was born in Jhenaidah, Bangladesh in 1996. He is completing his B.Sc from Military Institute of Science and Technology (MIST). His major of study is Computer Science and Engineering. Cyber security is the field of his final year research work. He has keen interest to work regarding cyber and network security. He has completed several projects related to AI, Computer Interfacing, Computer Graphics, Database Management System, Android Apps Development. Shusmoy has completed courses on Cisco Certified Network Associate (CCNA) and Mobile Apps Development. He attended 2nd IEEE International Conference on Communications and Photonics (ICTP), International Humanitarian Technology Project Competition (IHTPC) in Bangladesh University of Engineering and Technology.

Khandaker Annatoma Islam was born in 1994 at Dhaka, Bangladesh. She is a final year student in Military Institute of Science and Technology (MIST). She Her research interest is in Cyber Security, Computer Networking and Computer Interfacing. Her projects include automated electricity bill monitoring system in Interfacing, 3D DX-Ball in Graphics. She has a certification on Mobile Application Development Course, Arduino Microcontroller and Robotics Course.

Tania Tahmina Jui was born in 1995 at Pabna, Bangladesh. She is a final year student of MIST on department of computer science and engineering. Her projects include Computer graphics, computer networking, artificial intelligence, web development and data management. She also has a certificate on CCNA in computer networking.

Suzzana Rafi was born in 1993 at Dhaka, Bangladesh. She is a final year student of Military Institute of Science and Technology (MIST) in Department of Computer Science and Engineering. She has interest in Computer Graphics, Computer Networking and Artificial Intelligence. Her projects include creating a short animation in 3ds max in Graphics, a smart menu system in AI. She also has a certificate on CCNA in Computer networking.

Md Afzal Hossain was graduated from Bangladesh Institute of Technology (BIT), Rajshahi from the department of Electrical and Electronic Engineering (EEE) securing 1st class. He obtained M.Sc (EEE) degree from Bangladesh University of Engineering and Technology (BUET). He is pursuing PhD (in engineering) in the field of Multicore Optical Fiber (MCF) at BUET. He has obtained MBA (MIS) degree from IBA (Dhaka University) and M.Phil degree in National Security and Strategy from the University of Madras, Chennai, India. His fields of research interests are 'Optical Fiber Communication' and 'Information System Security'. He has a good number of publications in his credit in national and international conference proceedings and journals. Mr. Hossain attended the 12th ICACT (2010) in Phoenix Park, South Korea to present his research paper. Currently Afzal is serving as Senior Instructor (professor) in the Department of CSE, Military Institute of Science and Technology (MIST).

Ishraq Haider Chowdhury was born in 1993 at Dhaka, Bangladesh. He is a final year student of Military Institute of Science and Technology (MIST) in Department of Computer Science and Engineering. He has research Interest in Image Processing, Computer Interfacing and Artificial Intelligence. His projects include controlling intensity of light in a room using artificial intelligence. He also has a certification on Mobile Application Development.