JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Technology Based Crimes: Challenges and Way Forward

Bashir Ahmed

ABSTRACT

Technology based crime, also referred to as cybercrime, has increased in severity and frequency in the recent years and because of this it has become a major concern of attention for the companies, universities and organizations. Cybercrime refers to criminal activities that specifically target a computer or network for damage or infiltration. Cybercrime also includes the use of computers as tools to conduct criminal activity such as Internet extortion and Internet fraud. Computers significantly multiply the criminal's power and reach in committing such crimes. The governments across the world, police departments and intelligence units have started to react to cybercrimes. This study provides an overview of cybercrime and examines awareness in different respondents on the issue of cybercrimes in Bangladesh as well as emphasizes the severity of the problem and the urgent need to limit its impact worldwide. It is pertinent to mention that without creating a precise legal framework enabling law enforcement agencies to identify cyber offenders and prosecute them it is almost impossible to prevent cyber-attacks and cybercrimes in Bangladesh. The present technical protection measures in the prevention of cyber-crimes in the country there are many circles and cases wherein such technology is not available or failed or circumvented by a number of barriers. To remove all such obstacles, the existence of a proper legal frame-work is of great importance for recreating and maintaining cyber-security.

Keywords: *Cyber Crime, Law, Internet Crime, Awareness, Prevention.*

INTRODUCTION

The socio-economic development of any country is highly dependent on Information and Communication Technology (ICT). Considering the fact, the Government of Bangladesh is appreciatively turning the country into digital form and attaining the Vision 2021. Along with the success, this is radically contributing to another new form of crimes: ***Technology Based Crimes or Cyber Crime*** wherein the core of ICT, i.e., computer is used as an instrument of crime commission (Moore, 2011). The term Cyber Crime 'is conceptualized by the technical experts, police, lawyers, criminologists, and national security experts differently and increasingly unclear whether cybercrime refers to legal, sociological, technological, or legal aspects of crime and a universal definition remains elusive (Brown, 2015). It is tough to frame the fundamental characteristics of cybercrime with limited consensus. **Goodman and Brenner (2002)** opined this technology-based crime as the abuse of ICTs by criminals which is interchangeably referred to as **cybercrime**, **computer crime**, **computer misuse**, **computer related crime**, **high technology crime**, **e-crime**, **technology-enabled crime**. Terminologically, Cyber Crime is that **umbrella** which encompasses computers and technologies of all forms including internet, etc. for committing crime in the cyberspace. Hacking, digital child pornography, identity theft, intellectual property theft, and online fraud are the most diversified high technology-based computer crimes.

Technology based crimes encompass a wide range of activities, which may be divided into two broad categories:

1. Crimes which target computer networks or devices such as virus attacks and Denial-of-Service (DoS) attacks; and
2. Crimes which use computer networks to advance other criminal activities such as cyber stalking, phishing and fraud or identity theft.

PROBLEM STATEMENT

By moving forward into the 21st century, individuals are exclusively being dependent on the automation with the advent of technology which is highly noticeable in all spheres of our daily lives4. However, this development is also being viewed as the Doubled-*edged Sword* as whilst the technology has opened doors to enhanced conveniences for many, the same technology has also opened new doors for criminals and have been used to the advantage of the criminal fraternity. These crimes are popularly known as cybercrimes or, technology-based crimes or, **Cyber Dependent Crimes or Cyber Enabled Crimes** which are rising as a growing concern. Cyber Crime or Technology Based Crime is any violent action that being conducted by using computer or other devices with the access of internet. The enhanced use of ICT is boosting the hazard of cyber-attacks across the globe along with Bangladesh. Following Four major categories of cybercrimes are mostly found in Bangladesh:

1. **Crimes against the person** such as hacking Facebook account, etc.;
2. **Crimes against the property** such as extortion through using mobile phone etc.; and
3. **Crimes against the government** such as threatening the Bangladesh Government through using Facebook, Twitter, etc. by terrorists, etc.
4. Crimes against the society at large.

Over the past decade and more, Digital Bangladesh has been front and center of all our development. While the benefits of transforming into a digital economy cannot be stated enough, as more and more of our institutions embrace digitalization, the very real threat of cybercrimes must not be ignored. It was just witnessed a scare of a possible hacking attempt, with the central bank alerting banks to restrict online transactions and reduce ATM activity. While restricting or ceasing operations for safety reasons is an adequate response, the best way to deal with the increased threat of cyber-attacks is to simply strengthen our information systems. The ***under-reporting*** of cybercrime is also a serious problem, hampering the disruption and prosecution of cybercrime. In this regard, **Islam, Khatun and Paul** (2012) found that the most common reasons for non-reporting are negligence to crime, unwillingness of victims to report and fear of publicity.

OBJECTIVES OF THE STUDY

The objectives of the study were as follows:

1. To know the existing pattern of Technology Based Crime in Bangladesh;
2. To find out the recommendations for prevention and investigation of technology-based crimes.

JUSTIFICATION OF THE STUDY

In Bangladesh, as well as other commonwealth countries Technology Based Crimes and/or Cyber Crimes are not new phenomena. As this is quite impossible to frame the boundary of cyberspace, thus cybercrimes are posing significant threat to the law enforcement agencies gradually. However, internationally as well as nationally study on cybercrime with the problems and recommendations is popular concept but the discussion on this specific issue is a need to be discussed again and again in both academic and empirical area until this problem is solved. In addition, the problematic aspects of technology-based crime with problems and recommendations need a strong policy response. For that, the main purpose of the study was to know the existing crime patterns and explore the problems of and recommendations to combat.

THEORITICAL FRAMEWORK:

Technology based crimes or Cybercrimes are such criminal activities which involve an information technology infrastructure, including illegal or unauthorized access, illegal interception and data interference by unauthorized damaging, deletion, deterioration, alteration or suppression of computer data, and systems interference, misuse of devices, forgery, online threatening, and electronic fraud. In short, it is unlawful act wherein the computer is either a tool or a target or both. It includes with Cyber Bullying, Online Fraud, Identity Theft, Computer and Smartphone Fraud, Online Dating, Social Networking and Online Identity Monitoring, Social network fraud and solicitation, Virus propagation, Libel, Defamation, Data mining, Phishing.

Dr. Devamati Haldar and Dr. K. Jaishankar defined cybercrimes as such- “Offences that are committed against an individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly using modern

telecommunication networks such as internet (chat rooms, emails, notice boards or groups) and mobile phone (SMS/MMS).''

Maruf, et al. (2010)4 in the study titled **Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies,** discussed emerging cyber threats in Bangladesh with its brief history from late 1995 to 2006. The definition, characteristics, trends, types and patterns of cybercrimes were also discussed in the paper which includes Cybercrime against individuals, property, organization and society at large. The most common cyber-attacks and crimes were listed in the Present Scenario of Cyber Crime in Bangladesh section. At the end part of the paper available remedies for cyber or technology-based crime and their lacking consistent with ICT (Information and Communication Technology) Act, 2006 are recapitulated in the perspective of Bangladesh. It also illustrated some new dimensions as remedy against cybercrime like constitutional safeguard, special wing of police, and cybercrime agency by government, watch dog group, and public awareness. However, this study does not cover any statistical analysis and information about the rate of technology-based crime in Bangladesh but it discussed the all types of crime where computer and technology is used which is necessary for this study.

Hargreaves et. al. (2013) in the study titled as **Understanding cyber criminals and measuring their future activity** had drawn upon the discussions held in the workshop on defining a cybercrime and understanding the role by which the use of technology enables the criminal. They proposed a classification assessment to differentiate between the two fundamental categories of cybercrime: computer enabled and computer dependent crime. They explored the current state of information held, offering a data source taxonomy to facilitate the understanding of these datasets and identify the prominent features to aid data selection. During the workshop it was identified that in order to move forward in our research on cybercrime, an effort to standardize data must come into effect. The theoretical suggestions raised in this area are discussed along with how the information can facilitate research. Furthermore, they detail the key points of contact at which valuable data can be collected along with current and advanced mechanisms by which information could be obtained. Following the accumulation of data and its increased quality heightened research can begin. They therefore converse proposed research on both cybercriminals and their victims.

Mia, Badshah. (2015)6 in the study **Cybercrime and its impact in Bangladesh: a quest for necessary legislation** discussed the impacts of cybercrime in Bangladesh especially focuses on the area of personal life, workplace as well as Policy making Bodies or thinkers. He discussed types of cybercrime with the profile of cyber criminals and victims such as Hacking, Virus Dissemination, Software Piracy, Pornography, Credit Card Fraud, Sale of Illegal Articles, Online Gambling, Intellectual Property Crimes, Email Spoofing, Cyber Defamation, Cyber Stalking, Email Bombing, Data Diddling and Salami Attacks etc. and reasons namely Capacity to store data in comparatively small, Easy to access, Complex, Negligence and Loss of evidence etc. It also describes the impact of cybercrime against individuals and properties, organizations, governments, governmental and non-governmental organizations in Bangladesh. In the part of legal responses of cybercrime in Bangladesh it finds out some limitation of Information and Communication Technology Act-2006 and ICT (Amendment) Act-2013 where several clauses against cybercrime have but there is a chance to become safe side after committing crimes. So, considering these facts they proposed to impose a comprehensive Cybercrime Protection Act. However, although it contains lots of information about cybercrime in Bangladesh but don't have any statistical data, it is fruitful for my study.

Sreenivasulu and Satya Prasad, PhD (2015)16 in the study **"A Methodology for Cyber Crime Identification using Email Corpus based on Gaussian Mixture Model"** explained a novel methodology for email forensics and is highlighted using the concepts of data mining, semantic ontologies and Gaussian mixture model. The outputs derived are tested against accuracy using metrics like FAR and FRR. The results derived are presented above and revealed that the proposed methodology possesses high false acceptance rate and low false rejection rates. This methodology can be very useful in identifying from email corpus and thereby helping to identify the law breaker. Mixtures of data mining models along with the related methodologies are proposed in this paper to facilitate the email forensic assessor. The Performance is evaluated using False Rejection Ratio (FRR) and False Acceptance Ratio (FAR). However, this study does not contain all methods and techniques used in committing cybercrime and only explores email forensics rather it describes two methods which is helpful for present study.

Karim (2016) found in the study titled as **Cyber-crime Scenario in Banking Sector of Bangladesh: An Overview** a conceptual framework regarding the problem of cybercrime in the banking sector of Bangladesh by assessing the cyber-crime scenario. It shows some crucial statistical data of the cost of cybercrime in banking sector across the globe which is collected from FBI. It also reveals some case studies of cybercrime in the banking sector of Bangladesh like hacking of Islami Bank Bangladesh site by Human Mind Cracker, breaching the network security of Sonali Bank by Muslim Hacker, skimming attacks in six ATM booths and stealing $101 million from the Bangladesh bank's account with the Federal Reserve Bank of New York. The purpose of this study is to represents the concept of the basic crimes occurred in banks and financial sector- namely Automated Teller Machine (ATM) frauds, E-Money Laundering etc. The study found that by applying the updated technology and appointing skilled manpower and devices cyber-crime can be reduced from the banking transactions.

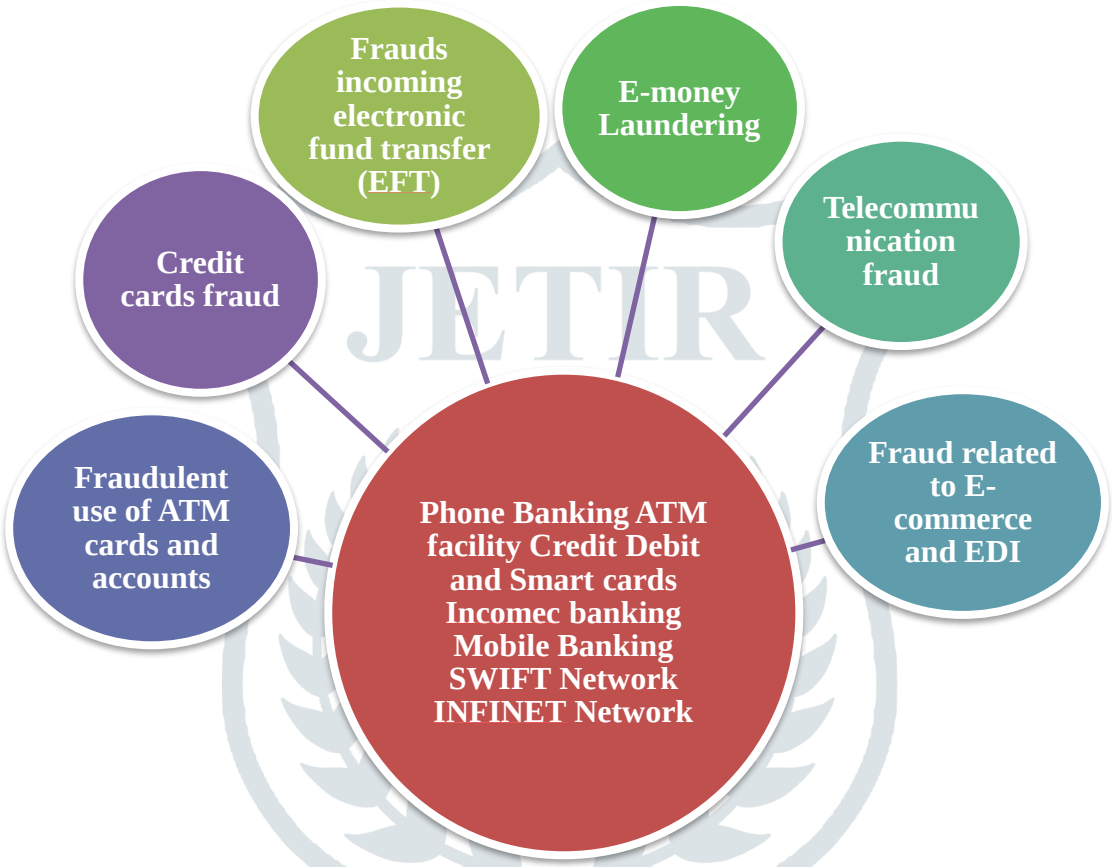

Figure 1: Technology & related crimes

Acts/Policies Deals with Technology Based Crimes in Bangladesh;

Crime is an intentional violation of criminal law which is committed without any defense and penalized by the state. To combat crimes as well as technology-based crimes, the Government of Bangladesh has formulated following legislative instruments and enacted laws for the law enforcement officials which are as below:

1. Information and Communication Technology (ICT) Act, 2006 (amended in 2013)
2. Pornography Control Act, 2012
3. National Cyber Security Strategy, 2014
4. Information and Communication Technology (ICT) Policy, 2015
5. Information Security Policy Guidelines, 2014
6. Digital Security Act/2018
7. Bangladesh Telecommunication Act, 2001
8. The Penal Code, 1860
9. The Code of Criminal Procedure (CrPC), 1898
10. The Evidence Act, 1872
11. Anti-Terrorism (Amendment) Act, 2013
12. The Constitution of Bangladesh (16th Amendment)
13. ICT Policy 2018.

CONCEPTUAL DEFINITION FOR THE STUDY

Cyber Bullying	:	A term used when describing a person who harasses, humiliates, intimidates, threatens, or embarrasses another person, either directly or indirectly through an electronic device such as the internet, or mobile phone
Hacking	:	The unlawful access of another's computer without the legitimate owner's permission.
Phreaking	:	The theft of telecommunication services such as phone phreaking
Identity Theft	:	The theft of another's personal identity, credit identity, or physical identity. It is labeled as the fastest growing high-technology crime (Moore, 2011)1.
Internet Fraud	:	The illegal fraudulent activities using online or virtual path as the medium of modus operandi.
Online Dating	:	The path by which someone wants to cause anyone harms, or borrow money from her/him through the online dating sites.
Online Harassment and Cyber stalking	:	The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.
Intellectual Property Theft and Digital Piracy	:	The robbing of people or companies of their ideas, inventions, and creative expressions known as intellectual property which can include everything from trade secrets and proprietary products and parts to movies, music, and software.
Cyber-terrorism	:	A relatively new term that refers to the way by which an individual who uses his or her hacking ability to instill a sense of fear in the public.
Virus Dissemination	:	The attack which causes for data loss, deduction of bandwidth speed, hardware damage etc. Trojan Horse, Time Bomb, Logic Bomb, Rabbit is the malicious software
Email Spoofing	:	A spoofed email is one that appears to originate from one source but actually has been sent from another source. Due to email spoofing personal relationship may be jeopardized.
Cyber Defamation	:	With help of computers and/or the Internet when any defamation takes place.
Email Bombing	:	Sending huge number of emails to the victim results in the victim's email account (in case of an individual) or mail servers (in case of company or an email service provider) crashing.
Data Diddling	:	Altering raw data just before it is processed by a computer and then changing it back after processing is completed. Government offices may be victims to data diddling programs inserted when private parties were computerizing their

systems.

Denial of Services (DoS) : An act by the criminal, who floods the bandwidth of the victim 's network or fill his or her email box with spam mail depriving him or her of the services he is entitled to access or provide.

METHODOLOGY OF THE STUDY

1 Study Methodology

To conduct the study used both quantitative and qualitative approaches to collect pertinent information from the wide range of stakeholders including victims of reported and non-reported criminal statistics, Police officials and NGO and GoB representatives. Study related data and information was collected through Unstructured telephone Interview and KII was done with the stakeholders, Observation (Overt & Covert), Analysis of Media (both print and broadcasting).

2 Conceptual Understanding

2.1 Crimes under the Study

The word Crime is derived from the Latin word *Crimen* 'meaning accusation 'or fault 'is an intentional violation of criminal law or penal code, committed without any defense and penalized by the state. For the purpose of fulfilling the study objectives, the study only focused on the **Technology Based Crimes**, especially crimes committed under the **Information and Communication Act**, **2006** (amended in 2013). For ensuring availability of **direct victims** for the victimization survey, the study avoided the *Cyber Pornography* under **Cyber Pornography Act, 2012**.

2.2 Victim of Reported Crimes

Victim of reported crimes refers to those victims who filed their cases with the police station to get justice.

2.3 Victims of Unreported Crimes

Victim of non-reported crimes refers to those victims who did not file and/or compelled not to file their cases with the police station to get justice.

3. Study Methods

"Research Design'' is the blue-print of any study. However, the main focuses of this study were to know the existing pattern of Technology Based Crimes in Bangladesh, comparative study to combat technology-based crimes by different countries through their law enforcing agencies, know the problems to combat technology-based crimes and derive recommendations for investigation, prevention and control of these types of crime. Simple random sampling is the primary sampling method used when selecting the sample for interview and KII. Both qualitative and quantitative techniques (mixed method) applied to ensure the fulfillment of the study. Information was collected both from primary and secondary sources. During data collection, consulted with the CID to collect their valuable comments, feedback, guidance and advice for the study. A desktop review of secondary data and documents was conducted which presents an overall idea about the present situation of all the result indicators. Overall, the study incorporates document search, field visit and data collection, data management, analysis and final report writing.

4.1 Review of the relevant documents

Secondary information was collected by consulting existing literatures and other published reports and documents including the documents of CID and internet search. The review work was done following a standard format with the view to gain better understanding about the projects and related activities. The following documents were consulted for the study:

1) Kegel, A. (July-December, 2016). Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates.

2) Sreenivasulu, V. and Prasad, PhD, R. Satya (May 2015). A Methodology for Cyber Crime Identification using Email Corpus based on Gaussian Mixture Model.

3) Brown, C. S. D. (January-June 2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology, Vol. 9 Issue 1.

4) Mia, B. (2015). Cybercrime and Its Impact in Bangladesh: A Quest for Necessary Legislation.

5) Risingbd.com (2015). Cybercrime in Bangladesh: A growing threat in digital marketplace.
6) Wall, Professor D. S. (October 2015). The Changing Cyber-Threat Landscape and the Challenge of Policing Cybercrimes in the EU.

4.2 Primary data collection

4.2.1 Study population

Study population were the victims both of reported and non-reported crime statistics, police administration, local administration, Officer in-Charge (OC) and Investigation Officer (IO) of the respective Thana, Case file officer, Duty officer, Cybercrime officer, high and mid-level cybercrime officials of CID, NGO and Gob representatives and members of civil societies including academicians, etc. Moreover, sources of getting victims were followings:

SN	Categories of Victims	Sources
1	Reported Victims	✓ Police Statistics
2	Non-reported victims	✓ Park, ✓ Market place ✓ Bus stand ✓ Cyber Café ✓ Universities ✓ Shop of Bikash Agent, etc.

4.2.2 Field data collection

1. Key Informant Interview (KII)

KII checklists were used for data collection from the respondents. All together 25 KII was conducted with the stakeholders of respective metropolitan police areas, which are presented in the following **Table 1**.

Table 1: Sample Distribution of Key Informant Interview for the Present Study

Tool	Respondents	Sample Size
KII	1. Officer in-charge from DMP	2
	2. Investigation Officer from DMP	2
	3. Officer in-charge from CMP	1
	4. Officer in-charge from SMP	1
	5. Investigation Officer from SMP	1
	6. Officer in-charge from RMP	1
	7. Duty Officer from BMP	1
	8. Duty Officer from KMP	1
	9. Duty Officers from DMP	3
	10. ASP/ADC from DMP	1
	11. CID Officers who deal with Cyber offences	2
	12. RAB Officers	1
	13. PBI Officer	1
	14. Journalist	5
	15. Lawyer	1
	16. Member of Civil Society (Criminologist)	1
	Total	**25**

4.5 Data Analysis:

For the present study, quantitative data was analyzed by using SPSS and MS Excel in light of the study objectives. The qualitative data was also analyzed in light of the study objectives by following three data interpretation techniques, like content analysis, narrative analysis and discourse analysis (**Figure 2**). After data analysis, the final report has been prepared following the results of both quantitative and qualitative findings.

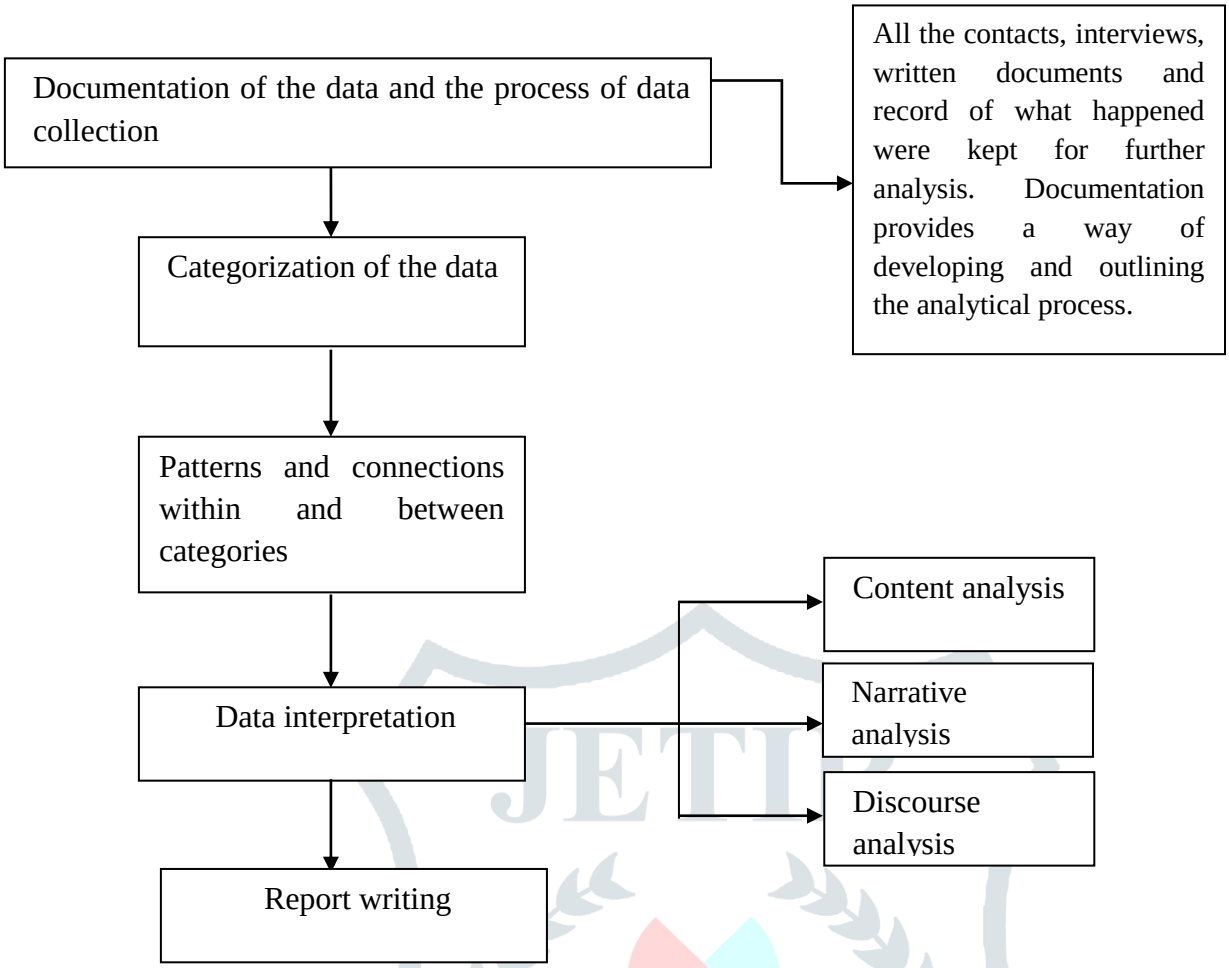

Figure 2: Qualitative data processing and analysis techniques followed for the study.

LIMITATIONS OF THE STUDY

A limitation identifies potential weaknesses of a study. Although, the study achieved the targeted objectives but there are a few unavoidable limitations.

The **first** is the **unavailability of the reported victims** and thus the study team did not get the predicted number of samples.

The **Second** is the **time limit;** the study has been conducted within three (3) months. Therefore, to generalize the study results for whole Bangladesh, it was required to involve more participants from different districts.

The **third**, victims' **readiness in participation or disclose information** was another issue. Thus, it was quite difficult for identification of the victims and collection of data and information both from reported and non-reported crimes, police officials, etc. Most unfortunately, the bank representatives, HR/NGO representatives, managerial officer of Mobile Company, etc. could not disclose detail information.

RESEARCH FINDINGS

1. Technology Based Crimes in Bangladesh

Generally, technology-based crime is a term used to refer to a loose set of frauds or abuses in which technology-based data or software play a major role. The study found several major categories of technology-based crimes which are: cyber bullying, hacking, cyber threatening, financial fraud, providing vulgar message, publishing nude picture and morphing, defamation, fraud by offering job, and use of electric device for copying (**Figure 3**).

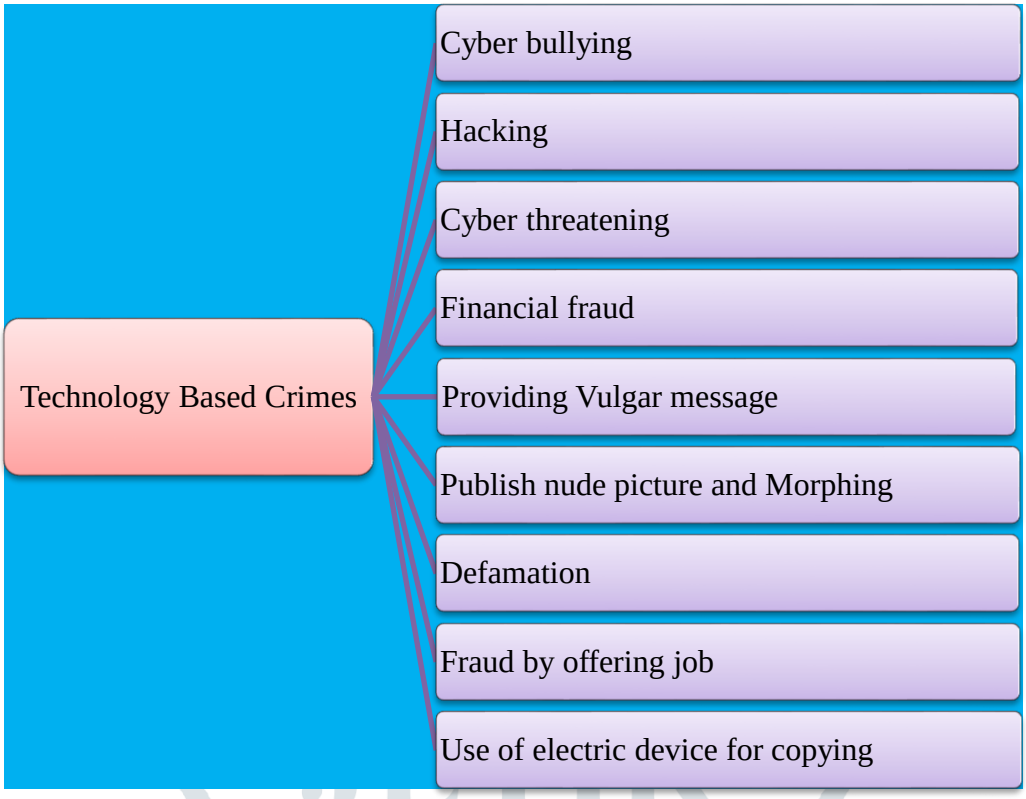

Figure 3: Major categories of Technology Based Crimes

In case of **unreported** cases, hacking was the mostly happened technology-based crimes which were in several forms such as hacking Facebook ID/messenger and sending nude MMS, nude post and unauthorized access through hacking email ID for business purpose. Cyber bullying was another form which remained hidden mostly, especially bullying through opening fake Fb account and bullying in social network by own account. A similar finding was there from the key Informants interviews. **Mr. Kamrul Ahsan,** an Additional SP of Cybercrime Center of Bangladesh police opined that there were three most occurring technology-based crimes: *cyber related crimes, financial fraud and financial/economic crime.* **Md. Shah Alam**, a DIG ofCyber Crime also accorded these crimes along provided a list of following examples of *financial crimes* occurred by mobile phone.

In the first two weeks of April 2020, there was a rise in ransom ware attacks, in which users have to pay money to get their computer to work again. It typically involves the sending of sham emails, saying that you have won a lottery, somebody wants to put their money in your bank account for which they will pay you a hefty amount, or more recently, somebody wishes to tell you 10 ways of saving your loved ones from the coronavirus. At present, Covid-19 has made many the primary targets of these crimes, because of their vulnerabilities and fear. The most common cybercrime that has increased during the pandemic, most likely, is phishing. As for laws, although phishing has not been specified as cybercrime in any statute, Section 24 of the Digital Security Act 2018 (DSA 18) in Bangladesh makes identity fraud or being in disguise an offense, indicating that those who steal people's information for later abuse will be punished for identity fraud, or for masquerading as victims. Since Covid-19 has pushed all businesses to shift their brick-and-mortar infrastructure into the cyberspace, e-business competitors are only increasing, leading to a surge in these crimes.

According to cybercrime center List of *financial crimes* occurred by mobile phone: are as follows:

- Financial fraud by *Hello Party or, Welcome Party*.
- Financial fraud by *Jean Er Badshah*
- Fraud by providing job or dealership
- Hundi business abroad by making the Bangladeshi captives
- Financial Fraud and
- Financial fraud by fake flex iLoad
- Fraud by using *Clone SIM or Clone like SIM* in three ways:
- By using Website
- By making last similar 6 digits

- Financial fraud by giving commitment to increase the marks of the public examination.
- Financial fraud by being fake Operator and using Baksh
- Terrorist activities, etc.

CONCLUSION

In Bangladesh, Technology Based Crimes and/or Cyber Crimes are not new phenomena. As this is quite impossible to frame the boundary of cyberspace, thus cybercrimes are posing significant threat to the law enforcement agencies gradually. The problematic aspects of technology-based crime with problems and recommendations need a strong policy response. For that, the main purpose of the study was to know the existing crime patterns. Cybercrime is obviously the latest form of the crimes which is very difficult to suppress. But its difficulty must not prevent us from taking adequate measures against the cyber-criminals. Only law is not enough and so, we must nurture ethics and morality in our private and communal lives. As our youngsters are prone to misdirection, they must be given proper guidance and care. The state has to take all possible measures to thwart any kind of cyber-invasion which may put the lives of people in danger. Continuous vigilance and upgrading counter-measures are some of the must-dos for the government. Common people should also be careful in using computer systems and online facilities. Hopefully, our awareness and constant battle against cyber-crime will result in success.

RECOMMENDATIONS:

From Stakeholders/Victims:

1. Stop biasness.
2. Corruption free police, prompt action and friendly behavior.
3. Try to make country terror free.
4. Find out actual offender.
5. Try to make country hacker free.
6. Emphasize on the opinion of general people, public service, awareness raising campaigning,
7. Establish justice, rapid punishment.
8. Awareness rising campaigning.
9. Should avoid powerful influence.
10. Social harassment
11. Should file case.

These are the most common recommendations from the general respondents.

Besides this, from the collected qualitative data during the study it can be said that Cybercrime Center and Investigation agency of our country should take necessary steps without delay.

1. MoU should be signed with Facebook, Google and Twitter etc.
2. Monitoring should be strengthened over various apps (Messenger, viber, telegram) etc.
3. To make competent Investigator and Supervising Authority Various Cyber related training should be given.
4. Establish division wise cyber–Police Station /Complain Center and Cyber Forensic Lab with skilled manpower.
5. Providing adequate Cyber Forensic/Investigation tools.
6. Use of Latest Technologies to detect and monitor the web-based communications.

REFERENCES

1. Gordon, G. R., Hosmer, C. D., Sidesman, C. and Radovich, D. (2003). Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime. US: National Criminal Justice Reference Service.

2. **Cyber-dependent crimes** can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware

for financial gain, hacking to steal sensitive personal or industry data and denial of service attacks to cause reputational damage

3. **Cyber-enabled crimes**, such as fraud, the purchasing of illegal drugs and child sexual exploitation, can be conducted on or offline, but online may take place at unprecedented scale and speed.

4. Kegel, A. (July-December, 2016). Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. International Journal of Cyber Criminology. Vol 10, Issue 2. Pp: 147-169.

5. NCA (National Crime Agency) (July 2016). NCA Strategic Cyber Industry Group: Cyber Crime Assessment 2016- Need for a stronger law enforcement and business partnership to fight cybercrime. Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/ file (accessed on April 17, 2017)

6. Gori, Dr. S. S. Cyber Crime and Its Impact on the Global Economy. International Journal of Law and Legal Jurisprudence Studies. Vol 1, Issue 8. Pp: 1-11.

7. www.cert.org/faq/cert_faq.html