CYBER CRIME IN PAKISTAN: DETECTION AND PUNISHMENT MECHANISM

A thesis submitted to Pakistan Institute of Development Economics in partial fulfillment of the final requirements for the degree of Masters of Philosophy in Public Policy

By

Ubair Anjum

PIDE2016FMPHILPP21

Supervised By:

Dr. Miraj-ul-Haq

Co-Supervised by:

Dr. Karim Khan

PIDE School of Public Policy

Pakistan Institute of Development Economics, Islamabad

2019

Pakistan Institute of Development Economics, Islamabad

PIDE School of Public Policy

CERTIFICATE

This is to certify that this thesis entitled: ***"Cyber Crime in Pakistan: Detection and Punishment Mechanism"*** submitted by Mr. Ubair Anjum accepted in its present form by the School of Public Policy, Pakistan Institute of Development Economics (PIDE), Islamabad as satisfying the requirements for partial fulfillment of the degree in Master of Philosophy in Public Policy.

Supervisor:

Dr. Miraj ul Haq
Assistant Professor,
International Islamic University, Islamabad.

Co-Supervisor:

Dr. Karim Khan
Associate Professor,
Pakistan Institute of Development Economics,
(PIDE) Islamabad.

External Examiner:

Dr. Anwar Shah
Assistant Professor,
School of Economics, Quaid-e-Azam University,
(QAU) Islamabad.

Head,
PIDE School of Public Policy:

Dr. Talat Anwar

ABSTRACT

Cyber-crime is an emerging phenomenon with technological advancement affecting each of the state. Cybercrimes are easy to commit, thus each of the country is dealing with the problem of cybercrime victimization and employing certain suitable measures to overcome of it. This current research study is Pakistan's based to evaluate "Cybercrime in Pakistan: Detection and Punishment Mechanism". As in context of Pakistan the issue of cybercrime is not being sorted out effectively and more of the incidents being occurred on daily basis. Women are being reported high being victims of the cybercrime as well as the specific age group is revealed to be highly victimized. The problem is becoming worsened due to the unawareness among people and the inadequate practice of the preventing measures within state. The students of the top ranked and high enrollment rate universities of Pakistan are the potential targeted respondents of the study. The data has been collected for this quantitative research study through online survey and the questionnaire was self-developed. Self-selection of the respondents has been adopted as the sampling technique of the study. The statistical analysis has been performed on this quantitative study and the verification of the hypotheses has been presented alongside the contextual support. The findings of the study reveal significant relationship of knowledge of cyber-crime, socio demographic factors and behavior of using internet with the ratio of cyber-crime victimization. The policy has been proposed based upon the results gathered and the support of the public policy theory. The final part of the study presents the recommendation.

Key Words: Cybercrime, Cyber victimization, Cyber Violence, Cyber Laws, Routine Activity Theory.

Table of Contents

ACKNOWLEDGEMENT

All the praises and gratitude is for ALLAH, WHO is most beneficent and merciful

First of all I want to acknowledge ALLAH Almighty, the superior and to whom all praises belongs. Without HIS mercy I would not able to complete my degree. HE gave me strength and power to accomplish my thesis so; I would become capable to complete my M. Phil degree with grace.

After ALLAH, my thankfulness and acknowledgment belongs to my parents. Their unconditional support backed me at each phase of education from the beginning. Their trust motivated me to work hard and to complete my thesis on time. My other family members also deserve acknowledgement as they had supported me in fulfilling my educational purposes.

My acknowledgement is of zero worth without crediting my supervisor Dr. Miraj-ul-Haq and co-supervisor Dr. Karim Khan. They gave their unending support, guidance, dedication and inspiration to me from the day first to the end of completion of this dissertation. They provide me critical feedback on each aspect of the research methodology and the subject matter of this study which made me competent enough to accomplish this research study which is the final requirement of completion of my degree of M. Phil.

DEDICATION

“My thesis is dedicated to my parents”

List of Tables

List of Figures

List of Abbreviations

CII	Critical Information Infrastructure
DDOS	Distributed Denial of Service
DRF	Digital Right Foundation
EIGE	European Institute of Gender Equality
FBI	Federal Bureau of Investigation
FIA	Federal Investigation Agency
MIT	Massachusetts Institute of Technology
NADRA	National Database and Registration Authority
ICT	Information and Communication Technologies
NR3C	National Response Center for Cybercrime
OECD	Organization of Economic Cooperation and Development
RAT	Routine Activity Theory
SPSS	Statistical Package for the Social Sciences

Chapter 1

Introduction

The overall domain of technology has been changed entirely after the www (World Wide Web) and online computer connectivity, which is considered mandatory for all aspects of business and corporate world. Before the internet revolution, both private and public organizations kept their highly confidential information in the form of physical documents. The physically stored information makes sure that the information is not easily available to anybody to take benefit from it, but their security was not much ensured. However, the new paradigms have generated huge data banks with all kinds of information rather than physical record keeping. Although the data banks is safer way to keep information as compare to physical record keeping, but all of the information which is available online even under strict security measures has the high risk of being attacked. Although this online available information could be the highly sensitive data of a country, personal bank details of the regular customers and the personal information of anybody. The reason of this risk is day by day advancement in technology and increased ratio of web users. Cybercrimes have diverse ranges and categories, thus the victims of the cybercrimes reveal to free of the age limits and the social backgrounds. Moreover, these crimes do not require expertise to commit; rather with the technological advancements the world has become global village and thus, the different ways to access the people easily across the globe and hacking their information have also been generated. In recent era everyone have an easy access to the internet but unfortunately this easiness have been used destructively as well, as more use of technology is

leading more cyber victimization. The people have 10 times higher threat of being victim of cyber-crimes as compare to the physical crimes.

1.1. Background of the Study:

The internet comprise of connected network of computers. This set of networks consists of millions of public and private computers having different users belonging to different backgrounds. All these computer nodes are part of different working groups that belongs to any organization or an individual. The technological grounds of new era based on the computers and internet has given birth to the common space for all human beings normally known as cyber space. Cyber space or commonly known as internet is the most used medium these days, in all aspects of human lives. It is involved in all domains whether it is business, entertainment, banking, education, logistics, military services or research. Virtually no human activity is possible without the usage of internet technologies (Crowther, A. 2017).

The development of society based on the internet technologies has introduced great advantage in all aspects of human lives. Flow of information across the globe and knowledge accessibility for common man has completely changed the face of modern society. Online shopping, online banking, voice over internet protocols for telephony services are a few examples of modern internet advancements. All these technical developments in the daily lives of common man have provided unhindered access to the information especially to the people from third world countries. With this level of information, the growth and advancement in society is facing a new and serious threat related to this zone. The information is now freely available on the internet. Most of the infrastructure like traffic control, water supply, air conditioning is completely

dependent on the internet connectivity and computer networks. So attack against these services and informational infrastructure may leads to disastrous and critical ways of harming.

For instance, Russell G., (2015) states that as a result of technological advancement the transition from paper money to the credit card devolution and seamless expansion of instantaneous and immediate global markets have completely transform the domains of crimes, and changes it beyond the perspective of place people and identity.

Other than technological advancement there are few other aspects of internet for those people who are using internet. Kemp, S. (2018), indicated that in 2011 one third of world's population near 2.3 billion people have accesses to the internet which have become 4 billion in 2018. Moreover, among 60% of these internet users belong to the developing countries and 45% of them have ages under 25. According to him, in 2017 the mobile broadband subscriptions reached up to 70% of the totals world population. He further estimated that, after the year 2020 the ratio of network devices with humans will be six to one. The more people on the internet from different backgrounds have increased the number of crimes through internet. These crimes are different from conventional crimes but their destruction is not less than the normal crime. Normally they are known as cybercrimes.

More cybercrimes left more victims as well. Every single person using internet is now having 20% more chances of being robbed through its computer as compare to the street robbing. Out of ten one adult is a victim of cybercrime. Hacking attacks and online frauds are just few examples related to the cybercrimes. All these crimes are committed on large scales and group of people with different technological backgrounds are involved in it who are normally experts of internet. Online fraud is the most prevalent form of crime as these days as compare to the normal theft. As

compare to conventional crimes, victims of cybercrimes are drawn from all ages, all backgrounds and all parts of world. As far as the gender is concerned it is also evident that women are more likely to be the victims of cybercrime as compare to the men. And effect of this violence has far more traumatic impacts on the lives of women as said by Jurgita Peciuriene, EIGE's program coordinator for gender-based violence.

1.2. Definition of Cyber Crime:

At present there is no common definition of cybercrime. Different terms like compute crime, technology enabled crimes, hi- tech crimes and cyber space crimes, all these terms are used interchangeably. The term is cybercrime is a broad term and encompass broader range of activities. For example hacking of state information, online child exploitation and theft of hardware also comes under the umbrella of cybercrimes.

Definition of cybercrime depends upon the specific domain in which it is being used. Certain limited number of actions performed against the violation of integrity and confidentiality of computer data can be considered as the core definition of cybercrime. Term cybercrime specifically referred to the crimes occurring over the internet or over the computer networks in earlier time, but later on this term has been converted to a generic terminology used for the computer crimes. Cybercrime is the third highly considered priority for the Federal Bureau of Investigation (Investigation, 2015). At the international level law enforcement agencies have found the increasing number of individuals and criminal groups involved in the cybercrimes. More than 80% of these criminal activities are well organized and concerned with groups. With the establishment of black cyber markets, these activities have become more organized and well

performed by creating malwares, bots and viruses for hacking the personal and financial data of people.

The term 'Cyber Crime' is as often as possible utilized as a part of 21st century information society and is a combination of two words 'cyber' and 'crime'. The terminology 'cyber' represents the internet i.e. virtual area with computer, in which different items knowledge and data is present; inclusively, the place where all the information can be manipulated and exposed to the rest of world. 'Definitions' of cybercrime for the most part rely on the motivation behind the aspect in which this term is being utilized. An illegal activity performed against the privacy, integrity and accessibility of computer based data and information or frameworks can fall into the category of the cybercrime. On the other hand, activities related to the computer used for individual or monetary benefit or damage, including types of identity related crimes and computer based content related activities do not allow effortlessly to define the complete terminology of cybercrime. Certain other complementary definitions are mandatory for the complete definition of term cybercrime. However the definition and pertinent of this term can be manipulated according to the scenarios in which they are using.

The terminology 'crime' encompasses multiple perspectives of society and considered as old as the origination of human culture. Crime is a legitimate wrong act that can be trailed by different procedures which may come in the form of punishments. According to Lord Atkin "the criminal nature of a demonstration cannot be found by reference to any standard however one, is the demonstration denied with punitive outcomes". As an idiom in criminology goes – "a crime will happen where and just when the opportunity benefits itself."

Until now, we knew about just conventional kinds of crime like murder, assault, burglary, blackmail, theft, and so forth. Now with the advancement and progression of science and innovation there appeared machines like computer also, offices like web. The web has opened up a radical new virtual paradise for the individuals excessive and terrible, sharp and credulous to enter and connect with parcel of various societies what's more, sub-societies, topography and socioeconomics. The extremely same ideals of web when gone in wrong hands or when misused by individuals with filthy personalities and vindictive aims, make it a virtual hell. Stories of copyright robbery, hacking and cracking, infection assaults and plain scams and so on have mounted up in the last few years. There is no single content accessible which gives a reasonable and predictable composition on the different classifications of digital crimes, their tendency, extension, highlights and basic fixings. It is important to analytically consider the cyber offences like cyber fraud, cyber terrorism, cyber pornography, cyber hacking, cyber ragging and cyber stalking to be fall in the category of cybercrime.

Despite of the fact that cybercrime is the term used frequently these days; it is hard to explain the term precisely because of its occurrence in multiple consequences. Like conventional crimes, cybercrimes can occur in numerous scenarios and have different facets. For example the council of Europe's Cybercrime treaty uses the term that refers to the criminal activity perform against the data content and copyright violation (brief., 2005). Zeviar-Geese, (2005) stated that cybercrime is a broader term and includes all the activities like child pornography, fraud, unauthorized access to the data and cyber-stalking. The manual of United Nation for prevention of cybercrimes consider fraudulent copying and unauthorized access to the personal data as a cybercrime (Nations, 1995).

Sarah & Ford, (2006), presents that cybercrime has two types; type 1 and type 2. Type 1 crimes are more technical in nature like bots Trojans or phishing scams. On the other hand, Type 2 crimes includes; sexual harassment, black mailing, planning terrorist activities online. These types of crimes are facilitated using different chat software (see Table 1.1).

Table 1.1: Types of Cyber Crime

Type No	Example	Software Used
1	Phishing scams	Email
1	Identity Theft	Trojan, key loggers
1	DDOS	Bots
2	Cyber terrorism	Chat software, Encryption
2	Cyber stalking	Messengers, Emails

Source: Sarah Gordon and Richard Ford, (2006)

McGuire, (2013) states that cybercrimes are violations, that can be carried out by using computer or any form of information technology. On the other hand these crimes can also be committed without using any technological domain such as cyber fraud is one of the type. Unlike conventional crimes, cybercrime can have bigger space; people from different backgrounds and different nations can be involved. While the impact of these crimes are also bigger and may range from one nation to multiple nations (Yazdanifard, 2011).

Enforcement of laws against cybercrimes is the area of lawful jurisdiction. Like contamination control representation, one nation can't without anyone else successfully authorizes laws that extensively address the issue of cybercrimes without collaboration from other countries. While the significant universal associations, similar to the OECD and G-8, honorably discussing about

the helpful plans, yet numerous nations don't share the criticalness to battle digital violations for some, reasons, including distinctive esteems concerning robbery or surveillance or the need to address all the more squeezing social issues. These nations, unintentionally or not, present the digital criminal with a place of refuge to work. At no other time has it been so natural to perpetrate a cybercrime in one local while holing up behind the purview of another. Despite the fact that the issue of purview in the internet can't be settled immediately, however still a worldwide exertion toward this path is the need of hour (Najam, A., and Bari, F., 2017).

1.3. Global Perspective of Cybercrime:

The revolution in the "www" (World Wide Web) has been witnessed in the economic downfall period, which increases the income variations, fixed private division spending, and minimized the money related liquidity. In last decades there is a dramatic rise in cybercrimes across the globe. As the more individuals and organized groups uses more disciplined attempts for these criminal opportunities for the sake of financial gains. Cybercrime executioner does not require any complex skills to carry out these activities. In developing countries normal people using computers have seen to be involved in the cybercrimes during their late teenage.

Crime prevention strategies comprised of the measures those minimizing the occurrence of crime and also mitigate the potential destructive impacts on people and society. Almost 40% of the countries have the policies and national laws designed for the prevention of cybercrimes. Rests of 20% countries across the globe are on their way to design the effective policies for prevention of cybercrimes. There are multiple dimensions of these policies based on different factors included educational level of people in country, law enforcement capacity of government,

leadership qualities and strong knowledge base of cooperation among private and government sectors. In many countries the cybercrime strategies are integrated with cyber security.

- It is clearly seen in last decade that the ratio of cybercrimes is more and more immense and this is one issue that should not be ignored in terms of its prevention. There are few statistical reports generated on this basis which is highlighted in this section:
- In 2016, cybercrime is the second most reported crime around the world (PWC, 2018)
- The ratio between the cybercrime and conventional crime has been increased. Nearly 50% of crimes are now cybercrimes (Agency, 2018).
- A cybercrime attacker keeps on monitoring the network for 146 days before final attack (Microsoft).
- Between April to June 2017 more than 11,000 people reports the cybercrime to the Australian Cybercrime Online Reporting Network (Now, 2017).
- Hackers are attacking the computers at continuous rate. Nearly there is one attack during every 39 seconds (Maimon, 2018).
- Most of network intrusions are caused due to the reason of insecure and compromised passwords (Blogs, 2014).
- Eighteen million new malware samples are captured during 2016 (Security, 2011).
- Data theft caused by security breaches was considered to be the major cybercrime with ratio of 91% (Corporation, 2013).
- The value of ransom ware also increases from $294 to $1,077 in 2017 (Corporation, 2013).
- The Netherlands has the lowest cybercrime rate in the world, while Indonesia has the highest cybercrime ratio.

Table 1.2: Countries with High Online Frauds

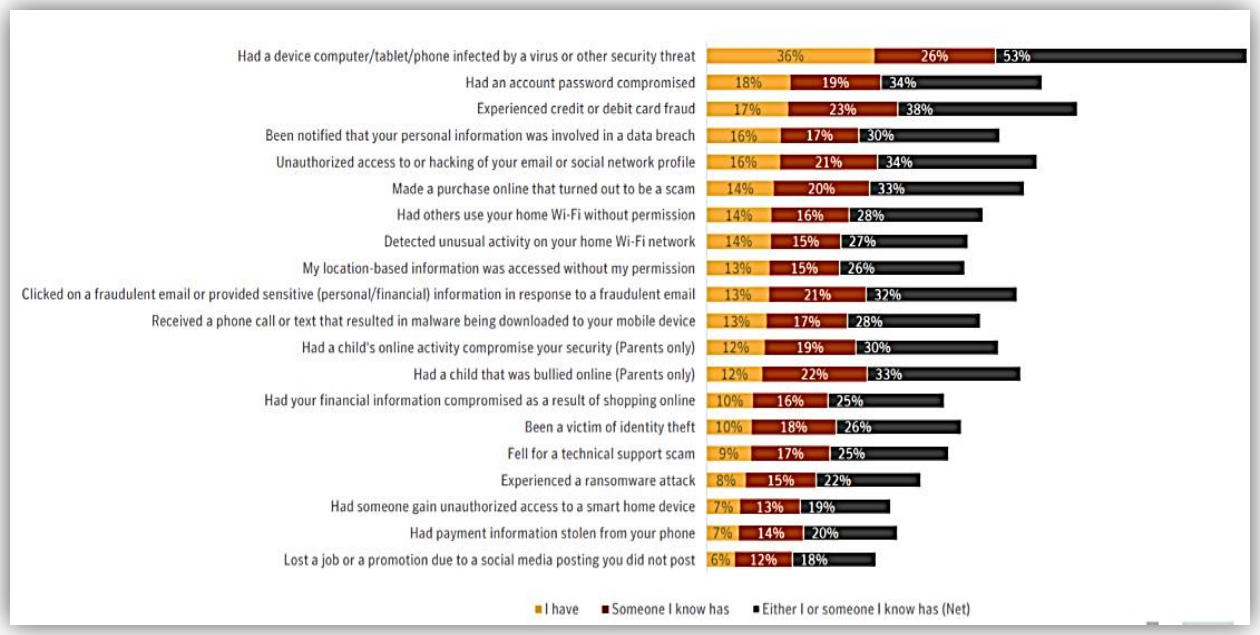
Top 20 Countries Victimized of Online Attack					
Sr.	**Countries**	**Total Attacks**	**Sr.**	**Countries**	**Total Attacks**
01	Canada	3164	11	France	368
02	India	2819	12	China	366
03	United Kingdom	1383	13	South Africa	349
04	Australia	989	14	Italy	291
05	Mexico	632	15	Pakistan	276
06	Russian Federation	594	16	Netherlands	266
07	Brazil	558	17	Malaysia	265
08	Germany	466	18	United Arab Emirates	259
09	Philippines	453	19	Spain	248
10	Japan	413	20	Argentina	238

Source: Adopted from Morgan, S. (2017). Cybercrime Report, 2017.

1.4. Victims of Cybercrimes:

In 2017 more than 978 million people globally from different countries experience any type of cybercrime. 53% of the online consumers are victims of cybercrime.

Figure 1.1: Norton Cyber Security Insight Report 2017



Cybercrime victims totally lost $172 billion globally. It is estimated that more than one million people are at the threat of being a victim of cybercrime on daily basis (Commission, 2018).This is really clear that people who are using internet have more chances to be victimized but there are numerous studies that shows that women are more victims of cybercrime as compare to men . Women are less safer as compare to men, as the executors of these crimes are not easy to capture for all the crimes they carried (Griffen, 2008). Cybercrimes against women are increasing at alarming rate as compare to men (Misra, 2010).

1.5. Types of Cyber Crimes:

Globally, cybercrime can be categorized into different domains which may include commercial driven crimes, and dishonest access of highly confidential data or content or any other activity that destroys the integrity and confidentiality of data stored in computer system. Currently,

statistics about the cybercrime do not provides the strong base for comparison of these crimes across the different nations. And these crime statistics are insufficient to make any conclusion about their seriousness but they can be used for the policy making and other procedures.

In this section different types of cybercrimes are discussed in detail.

1.5.1. Hacking:

This sort of offense is regularly eluded as an illegal access to the data in computer. This data can be personal information or it can be highly confidential information related to the military or sensitive assets of country. Hacking is the most common form of data stealing and used for the benefit of a hacker.

1.5.2. Information Theft:

This information theft can be done from different physical devices including computer hard drive, removable media etc. This theft might be performed by changing the information physically or by altering them through the other virtual mediums.

1.5.3. Email Bombing:

This type of activity send the large number of junk e-mails to the people, which might be an individual or an organization or even mail servers and it is possible that the e-mail servers may crash because of excessive emails.

1.5.4. Virus Attacks:

Viruses or worms are programs that affix themselves into a computer or a document and then move themselves to different documents and to another different computer in an organization over a network. They influence the information on a computer, either by changing or erasing it. Worms, not at all like infections, need the host to connect with. They simply make practical duplicates of themselves and do this over and over till they gobble up all the accessible space on a computer's memory. E.g. adore bug infection, which influenced the 5 % of the computers of the globe. The misfortunes were accounted to be $ 10 million. The world's most acclaimed worm was the Internet worm let free on the Internet by Robert Morris at some point in 1988. Nearly, conveyed advancement of Internet to a total collapse.

1.5.5. Salami Attack:

This type of crime is based on the financial aspects. A critical perspective of this kind of crime is that the modification in the system is so small that no one can notice it. For example, the Ziegler case in which ten pennies was deducted against every transaction and stores in a certain bank account. This deduction of ten pennies is not noticed as it was a small amount.

The knowledge of these kinds of cyber-crimes is necessary for this study in order to present the clear and particular representation of cyber-crimes, their occurrence and the victimization due to the certain category of the cyber-crime.

1.6. Research Gap:

The aforementioned section has discussed the background and the global perspective of cybercrime and reveals that the term cyber-crime is still being confused due to the different aspects of the occurrence of the cyber-crimes. Cyber-crime has been study out generally in most

of the studies without categorizing the victimizations in terms of the gender or age groups (Arfi and Agarwal, 2014). This inclusive research study has been carried out in order to clarify the category of genders in cyber-crime victimization specifically in the perspective of Pakistan. Though, there are so many studies in perspective of the developed states; Europe, United Kingdom and the United States of America concerning the cyber-crime but the changing trends and the living mechanism of states diversify the effects of cyber-crime victimization for each of the geography inclusively. The ratio that how many women victims have been target of cybercrime is not exact. Moreover, there are discrepancies in measures and initiatives by the Pakistan to deal with the issue of cyber-crime and to overcome of it, so it is a central problematic hallmark for the world as well. This current study will give an comprehensive analysis of the unfortunate victimizations in cybercrime and the distinctive preventive estimates that have effectively taken for ceasing the cybercrimes as well, by focusing the geographical region, "Pakistan", as the under study state is revealed to have increased issues of cyber-crime and insufficient approaches to overcome of this problem.

1.7. Scope of Study:

Investigating and dealing with the cybercrimes is a huge and complex task. These practices completely rely on the adaptation of effective practices in procedures, legislations, policies, resources and technologies. The Internet has enhanced the information transference and world has become global village so everything like internet banking, shopping, gambling all the information is present online, that's why more and more people have become the victim of cybercrime. This aspect of the internet has immensely enhanced the opportunity of cybercrimes for everyone. This study will critically analyze the awareness of people in context of cyber-crimes. It particularly focuses on the fact that why the rate of cybercrime is continuously

increasing and which age groups are the most victims globally and in context of Pakistan. Although the cybercrime is a vast terminology, but the laws and procedures applied by each country is different depending upon the different cultural, educational and economic aspects of the country. However, every country has different technological infrastructures against the cybercrime which sometimes impede the overall efforts of cybercrime. The study will also focus on the anticipatory measures that have been applied by the government of Pakistan in order to minimize cybercrimes.

1.8. Problem Statement:

The issue of the cyber-crime is increasing with the technological advancement and the accessibility of the internet in hands. The people those are more prone to be victimized of cyber-crime have diverse ages and genders. Pakistan's government measures to overcome of this harmfully effecting phenomenon are not sufficient. Thus, there is an utmost need to identify the group of people being more victimized by cyber-crime within the state and to propose the initiatives with and through advising a policy on cyber-crime to control and overcome of the problem. The students of the top ranked and higher enrollment rate universities of Pakistan have been targeted as the potential respondents of the study as they are the more web user population. The online survey technique has been employed for data collection in order to have higher respond rate with lesser surveying hindrance.

1.9. Objectives:

It has been identified in this study that, the knowledge of cybercrime is necessary to critically analyzing the cybercrime victimization. The categorization of the victims is necessary in terms of their ages and genders in order to unveil the certain group of people being more victimized and

then for sake of proposing the more focused policy for them along with the revealing the issues of occurrence of cybercrime in Pakistan and the limitations to overcome of it within state. In this context this study devoted to achieve the following objectives:

1. To analyze the terms related to cybercrimes analytically in different domains
2. To examine the genders differences of the cybercrime victims.
3. To examine the age group of the high cybercrime victims.
4. To investigate the internet using behaviors of the cybercrime victims.
5. To investigate the reasons of cybercrimes in Pakistan.
6. To identify limitations and problems faced by Pakistan while investigating cybercrimes.

1.10. Expected Outcomes:

This study is related to the "Cybercrime in Pakistan: Detection and Punishment Mechanism" and thus deals with the consideration and insights of cybercrimes and its detection in terms of knowledge, awareness, age group, gender, issues, limitations and its effects in domain of Pakistan. Contextual foundations revealed that the measures to deal with the negatively occurred phenomenon of cybercrime are not sufficient to resolve the issue. This study with identification and detection is about to disclose the root causes of occurrence of high ratio of cyber victimization and is about to present the policy ultimately on cybercrime and cyber harassment to resolve the issue within state.

1.11. Beneficiaries:

Since the study is about the cybercrime, which is most promising social issue of the era. The potential beneficiaries of this study are the cyber-crime victimized and common people of the state and crime departments by identification of the cybercrime's root causes, their potential

victimized and then providing the solution with and through the results and policy to restrict this social evil within state. The study after presenting the results and devising the policy on cybercrime is expected to serve the common people of the state, the policy makers and the practitioners as well as the crime departments to consider the issue at their extreme interest with the outcomes and implications of this study.

1.12. Organization of the Study:

- **Chapter 1:** Chapter one is comprised of 14 segments. The first portion present the introductory note of the chapter, the second portion explicate the background of the study. The lateral parts are in explanation of the rationale, scope of study, problem statement, objectives, proposed theoretical model, hypothesis, expected outcomes, and beneficiaries. While the last portion of the chapter presents the holistic structure of dissertation.
- **Chapter 2:** Chapter 2 it the chapter of literature review. It includes strong contextual backgrounds on global perspective of cybercrime, cybercrime victimization generally, cybercrime victimization in domain of Pakistan and limitations as well as problems faces by Pakistan in domain of cybercrimes.
- **Chapter 3:** Chapters 3 is the chapter of research methodology and present the overall research process. The chapter starts with the introductory note and then elucidates the research paradigm, research approach, research design, data collection procedure and techniques, data analysis and ethical consideration.
- **Chapter 4:** This chapter is the chapter of analysis and results. It provides the complete description of the results and interprets all of the results clearly and comprehensively. This chapter starts with the introduction. The tests of descriptive statistics of

demographic profile of the respondents and survey items were generated and interpreted. And then the hypothesis testing along with interpretations has been presented in this chapter.

- **Chapter 5:** It is the final chapter of this research report. This chapter discusses all of the results generated in previous chapter along with logics and evidences. Then this chapter presents findings, implication, conclusion, recommendations and proposed a policy on cybercrime under the light of the study. The final part of the chapter is conclusion. It presents the glimpse of the overall research study in the form of summary.

Chapter 2

Literature Review

2.1. Introduction:

This study is about to investigate "Cybercrime in Pakistan; Detection and Punishment Mechanism", thus deals with the investigation on the most primal social issue affecting the lives of a lot of people in Pakistan. In this context this chapter will cover the comprehensive review of studies on the subject of cybercrime and its victimization. To meet this objective this chapter have been comprised of six sections namely as, cybercrime; concept and typologies, worldwide vision of cybercrimes, cybercrimes victimization, cybercrime victimization in the perspective of Pakistan and limitations and the issues Pakistan is facing in regards of cybercrime.

2.2. Cybercrime; Concept and Typologies:

William Gibson originally exploited the term 'Cyber Space' in 1985 in one of his novel known as "Neuromancer". But now at present time this term has turned into far reaching range because of its excessive use (Jamil, Z., 2006). Recently Navneet, K. (2018), argued that any of the illegal and punishable acts by the establishments or the state is known as the crime, but in current scenario the most promising crimes are those known as cybercrime; the crime spreading recklessly due to the fastest emergent technology and its usage having the complicated investigation procedures due to the improper framework of the analysis and exploration. Cybercrime is a miscellaneous term and anticipates the multiple terminologies under its domain. Gordon, S. (2004), has presented two particular terminologies accompanying with the cybercrime; "cyber dependent crime and cyber enabled crime". The former one crime conducted with and through the engrossment of the computers or other forms of ICT; including the crimes

encompasses hacking, DDOS (Denial of Service) attacks or diffusion of malicious and mischievous software (McGujre, M., and Dowling, S., 2013). According to this study these types of the crimes performed directly in contradiction of network infrastructures or for other fraudulent purposes. On the other hand the lateral one, known as "cyber enabled crimes" are those resembling to the normal kinds of crimes but could be ameliorated by means of operationalization of ICT; such as frauds utilizing phishing tricks and media advertising, sexual badgering utilizing web or spreading sexual pictures using distinctive sites and so on and theft of data identified with bank and charge cards (McGujre, M., and Dowling, S., 2013).

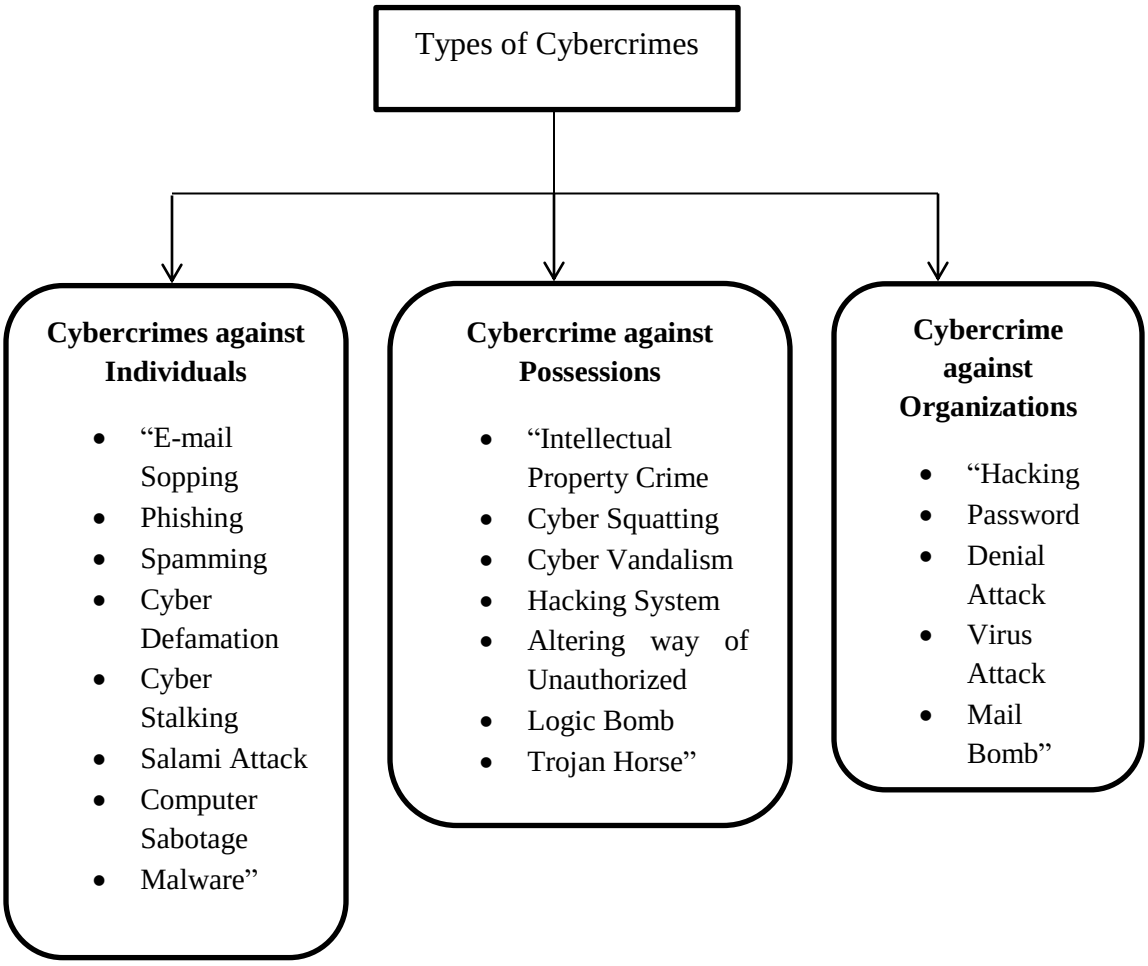
As indicated by Gordon S., (2004) a few cybercrimes needs highly advanced proficiency. For instance cybercrimes such as; DDOS, burglary of identity additionally require more and profound learning about the advanced digital technologies. It implies that cybercrimes change in definition relying upon the profundity and expansiveness of area where wrongdoing has been committed (Viano, 2006). Cybercrimes are not similar to those of conventional crimes, the differentiation of cybercrimes from the conventional crimes have four perspectives to include; (1) physical nearness is not required for their practice, (2) a very few assets required for such crimes (3) they are hard to arrange as their legitimate and unlawful definitions do not exist (4) there is no compulsion of specialized instruction so as to commit them as they are anything but difficult to succumb (Madhava, 2011). By considering these perspectives Kundi (2010) stated that these issues made the cyber security measures challenging to implement in developing nations. Here the phenomenon arouse if cybercrimes do not needed any physical existence then how these crimes practices and by whom. Halder (2014), on this portent states that cybercrimes are the wrongdoings which have been done by individual as well as group of people having criminal expectations. These crimes carried out against the individuals, associations and the

organizations in purpose to damage or harming them; for example hurting the unfortunate casualty physically and rationally who utilizes any type of media transmission network or social media. Moreover, this study stated that, cybercrime can be classified into two taxonomies fundamentally; in first classification cybercrimes infect the computer system of the casualty with and through some kind of software or malware, from the notion of second perspective the cybercrime have some aspects of conventional crimes for example fraudulent conducts and theft by means of computer and technological assisted advancements. From another perspective presented by (Holt, 2012), cybercrime has turned into the mindful issue on account of the day by day advances regarding the newfangled innovative domains. These innovations have made it complex to identify the sort of wrongdoing and locate the ill-conceived who are sitting miles away. Because of the extension of ICT new scares are appearing on ordinary bases and every day web client confronted with many of the difficulties, which is also a major risk to the security and wellbeing of any country. According to Wall, (2007) there is a difference between the "computer assisted" and "computer oriented" crimes. Former are those crimes which are completely based on the latest technology hence committed by using for example online resources. An example is the selling of bogus and online products online. Latter are the ones which are based on latest design and implementation like malicious software and viruses etc.

There are different types of cybercrimes discussed in literature, as presented in Navneet, K. (2018), there are three broader typologies of cybercrimes; cybercrimes against individuals (E-mail Sopping, Phishing, Spamming, Cyber Defamation, Cyber Stalking, Salami Attack, Computer Sabotage and Malware), cybercrimes against property (Intellectual Property Crime**,** Cyber Squatting**,** Cyber Vandalism**,** Hacking System**,** Altering way of Unauthorized**,** Logic

Bomb**,** Trojan horse) and cybercrimes against organizations (Hacking, Password, Denial Attack, Virus Attack, Mail Bomb).

Figure 2.1: Types of Cybercrimes



Source: Navneet, K. (2018)

On the other hand Smith (2010) has presented distinct names of typologies of cybercrimes as explained above but the essence of all typologies is same ultimately. According to Smith, (2010) there are three types of cybercrimes semantic, syntactic and blended. Semantic are the one related to the social networking where sometime users data that is present online is used for the

frauds. It also includes social phishing, spam emails etc. Syntactic are the ones which are purely technical, based on the malware and viruses and Trojan horses. Blended is the combination of both where normally a victim is being contacted and provided him with a solution in return of money or financial gains. In this case the personal information stolen from victims is sold and used for further frauds.

2.3. Worldwide Vision of Cybercrime

Technologies have ceased the geographical distances, online interaction or communication via web is the very significant practice in present day world. As Manjikian (2010) argued that, because of this kind of interactions individuals and associations allied over the system are confronting prominent danger of cybercrime. Cyber illegitimates are perpetually creating contemporary methods to get more data about the administration rather than the budgetary data having a place with the common man. According to the survey particularly in underdeveloped nations like Pakistan, this is a genuine danger because of less viable preventive measures. As indicated by I. W. Insights (2016), 51% of total populace has access of the internet or web. Before the finish of 2017 right around 3 billion individuals have an access to the web out of which 2.3 billion are from the developing nations including 89 million from most under developed countries.

The contraption of internet has brought lot of advantages to the society but it has hatched numerous opportunities for multiple online crimes on colossal scale (Button, 2013). All of these cybercrimes are not only restricted to English speaking countries by these criminals are

accessing other countries like Korea and Japan as well. Phishing scams and one click frauds are becoming common in these countries (Daily, 2013).

Among the twelve countries who are facing the highest ratio of cybercrimes ,eleven are from global south including Romania, Colombia, Indonesia, Thailand, Bangladesh, Iran, Zimbabwe, Saudi Arabia, Nigeria, Vietnam and Kenya (Kimberly J. Mitchell ∗, 2008). But the ratio has been changed according to the recent study of Morgan, S. (2017), presenting the list of top 20 countries being more victimized of cyber-crimes; Canada, India, United Kingdom, Australia, Mexico, Russian Federation, Brazil, Germany, Philippines, Japan, France, Chine, South Africa, Italy, Pakistan, Netherland, Malaysia, United Arab Emirates, Spain and Argentina. According to (Huff, 2010) cybercrime has become requisite part of some economies. For instance it is considered as the third biggest earning industry in Kenya. The most established and competent hackers in these economies are also enriching the cybercrime echo system. Some of these hackers have micro enterprises while rest of them belongs to hefty and more trained groups (Bryan-Low, 2012). Two economies with highest cybercrime victimization rates are South Africa and China (Norton, 2012).

McAfee, (2018) presented that, 85% of the global computer networks are accessible to the criminals and spy agencies. After the sophistication and rapid attacks of cybercrime increases numerous countries have designed and implemented cyber warfare capabilities (Markoff, 2010). A survey conducted with worlds top internet experts concluded that China has the highest capability of cyber warfare. While Russia is at second number with USA and Israel are third with combating capabilities against cybercrimes. The company RSA's credentials were hacked by the hackers from China in such a manner that company offers all new credentials to millions of its

consumers (Baker, 2011). POULSE, (2018) stated that, 66% of adult consumers are now worried about the cyber-attacks as compare to the physical crimes in US. According to Gen.Keith Alexander which is the commander of cyber command in US, cybercrimes based on the money theft are the greatest transference of wealth in the history.

Furnell, S. and Emm, D. (2017) have presented in their study that, Notpetya is the greatest ransomware hitting the associations in 2017. Notpetya was beyond the conventional ransomware since it is especially configuration to harm the framework of the state. Notpetya makes the loss of 300m dollars the Maersk. But it was not the only case of ransomware as Wannacry is another case in this lane which is utilized for fund-raising shorn of any technical capability (Chen, Q, and Bridges, R A. (2017). According to them, the essential focus of this Wannacry was medical clinics, drug stores and hospitals as well as surgeries. The yahoo assault impacts 3billion clients all around and considered to be the biggest unveiled hack ever of in cybercrimes. The expense brought about by these ransomware is required to surpass by 5 billion dollars in 2017 (Norton, 2012). Goodman, (2010) has presented that offenders behind the cybercrime can completely robotize their assaults because of which there is exponential development in the crimes and wrongdoing around the globe. But from all over the globe the developing countries considered as the center of the cybercrimes (Jaquire, V. and von Solms, B. 2015), as indicated by “Chris Rock” the organizations in Middle East, Africa and Asia are very easily accessed task for the hackers to do crime, because these organizations don't put more cash into cyber security prospects as having low budgeting. The greatest impacts of cybercrimes have been available in the developing nations as hackers have all the more proving grounds for their malevolent software (Dijk, J. V., 2007).

Kevin Mitnick (2011) in “Ghost in the Wires: My Adventures as the World's Most Wanted Hacker” notice that, individuals purchase the best mechanical protective instruments for success of their business systems and to spare them from hacking. Yet there is a danger of being a casualty of cybercrime on account of different security breaks in these apparatuses. As indicated by Zareen, M. S. et al., (2013) malware such as, “Disttrack and Stuxnet” unveiled that the internet is all the more roughly abused by the underdeveloped nations. Corporation, (2013), has been presented that the nations like South Korea, Egypt, Pakistan and Philippine are positioned amongst upper ten those nations which are associated with the inception of malware exercises.

Commercial Victimization Survey (Office, 2013b) presented that there is assessed 180,000 occurrences of cybercrimes happens over the four business segments which may incorporate assembling, transport and settlement. The cyber-crimes identified with computer viruses which have been diminished, but to the other side hacking has been extended or increased. It has been revealed from the survey that the prior proportion of the viruses originated threats confronted by the adults was no more than hacking, additional to this, in comparison to 2006 or 2007 this proportion has expanded by the ratio 2% in 2012 or 2013 and nearly 3% of adults ratio have reveal to lost their cash in these kinds of crimes (ONS, 2006).

2.4. Cybercrimes Victimization

Cybercrime victimization is getting intense research charm in last few years, especially online harassment is the most studied topic in this perspective (Jones LM, 2013). “Routine activity theory” (RAT) is considered as the theoretical and contextual framework applied in the domain of social sciences to determine the different aspects of cybercrime victimization (Cohen, 1979).According to (investigation, 2015) almost 288,012 cases of cybercrimes were reported in

USA; out of these 49% were reported by women. It is also noticed that the ratio of these crimes have been increased from in 2015 as compare to 2013. BBC World and GlobeScan Poll (2014) conducted a survey across seventeen countries. Results revealed that there is growing fear of insecurity among online users. Results of these polls show that media and internet are at risk. Results of survey show that France with 76%, Spain with 66%, Canada, USA and Germany with 65% ratio of people thinks that they are not able to express their opinions online. The majority of internet users in the EU 61% people are experiencing theft, 51% are exposed to child pornography accidentally, 49% faced online fraud and 48% are exposed to email scam. Out of these 41% people are scared of using online services because of theft and cyber-attacks. 38% of users have reported that they got emails on daily basis asking for money (Commission, 2018). 75 million emails are sent daily asking for money which generated 200 victims daily. Hence 72% of Americans have faced some form of cybercrime in their life (watch, 2011). 60% victims of cyber stalking are women. Most of these crimes are carried out by using Facebook accounts.

According to (Internet World Stats, 2015) Finns have the highest penetration of 97%, USA 86.9%, Germany 88.6%, and UK 89.8%. This rate plays an important role in potential exposure of people towards the victimization possibility. The comparison between the ratios of online harassment has been considered from year 2000 to 2010 in American youth. Therefore it is clearly seen that there is an increasing ratio in this context. On the other hand 11% of victims report about the online harassment by 2010 (Jones LM, 2013) . Personal traits, social relationships and demographic analysis can give greater insight about the victims of cybercrimes (Paternoster, 2011).

According to Dutch victim survey 2% of whole population have experienced threatening chat, sms and emails, while 6% has experienced offline threats from different offenders (Van der Meulen, 2010) . Millions of people have victims of frauds on daily basis all across the world. Thousands of fraudsters are operating from different countries beyond the borders of victim countries (A. B. o. Statistics, 2014). Online frauds have made more people open to the victims as compare to the previous era. Most of the times, these victims try to hide their experiences in order to save them from embracement. But research studies about these victims have shown that there is lot of beneficial information that can be gain from them (Huff, 2010)

New form of social interaction has been originated from Facebook which give rise to lot of cyber-crimes. Facebook launces in 2004 and right now it has 2.19 billion active users (Statista, 2018). These social networking sites have been used people for seeking the love so romance based scam has also increasing drastically. It is found that one in a five relation now starts online (Nolan, 2012).

Consumer frauds have not be reported by the victims in all cases. The reason for this is that victim wants to save him/her from embarrassment and self-blame. Same study in UK highlighted that only 44% of these victims have reported about their issues (Goucher, 2010). Hence there is no data about the fact that how many people have been victims of online frauds in last few years globally and specially in context of different countries. This research do not distinguish whether these crimes are committed online of offline (McGuire, 2013).

According to a survey conducted in 2016 in Australia, it is noticed that almost 70% of the women under age of 30 years has faced the harassment and abuse through online sources. Similar trend can be seen in all other parts of the world (Hunt, 2016). Another study analyzed

that both men and women are harassed online but the nature of harassment is quite different for the women. Women in all countries faced more intense and consistent forms of harassment. Women is harassed and stalked sexually more often online as compare to men (Duggan, 2014).

There are many of the studies based upon the phenomenon of the younger generation victimization of cybercrimes (Oksanen and Keipi 2013). According to the studies focusing on the young age cybercrime victimization the comparison has been plotted between the younger and the older generation in context of cybercrime harassment. According to the Wolak and Bulletin, (2006), the studies reveal the aspect that those people who interacted more to the online sources or web based activities on social media such as; chatting are more prone to be cybercrime victimized, as these individuals are all the more oftentimes on the web so, the probability of turning into a casualty of cybercrime. According to Wolak and Bulletin (2006), particularly the folks those progressively unpracticed in social exercises and effectively trust other individuals online have more opportunities to fall in the snare of cybercrime.

Most of the prior studies demonstrated that the young females or those having age between 18years to 25 are more prone to be casualties of sexual harassment and supplication as contrast with the men (Helweg-Larsen, 2012). Clemmitt (2006) explicated that most of the teenagers and the women hold a perception that the socialization on different social networking sites won't expose their actual identity and they could use them without any of the threats, so they attract more towards the different social sites; but they remained unconscious about the reality that such certain sites exposed their identity in an unwanted or bad way (Clemmitt, 2006) and the chances become higher that they moved toward becoming casualty of sexual harassment or theft as well as even can be face aggressive behavior at home by their ex-life partners (K, 2009). The general measurements and statistics of cybercrime casualties revealed more of the victimized as the

people of younger ages as compare to the other causalities. Oksanen, (2013) has been presented in his study that in 2008 inside the age range of 15 years to 74 years, about 2.5% individuals is accounted for as casualties of cybercrime. Howsoever, this proportion is about 5.3% amongst the age range of 15 years to 24 years.

Moreover, Wolak and Bulletin, (2006) have been presented that, 4% of Americans have been victimized of the cyber harassment. Statistical data taken from the report of 2012 demonstrated that just 10% of web clients have become the casualties of phishing or online tricks (Norton, 2012). But according to McKenna, (2000), there is another point of view validating those clients who are increasingly dynamic online, are more prone to be the victim of cybercrime as contrast with those less dynamic. According to this reality it is likewise significant, as the youngsters are progressively dynamic clients of most recent innovations as contrast with the elderly individuals (Ybarra, 2004). Staksrud, (2013) has presented that children who are all the more effectively utilizing internet based activities and are all the more effectively taking part in online maneuvers have more danger of turning into a cybercrime unfortunate casualty. As per Blogs, (2014) two out of three individuals have encountered a scam in most recent a year.

2.5. Cybercrime Victimization in Perspective of Pakistan:

Along these lines the cyber-crime oppression in Pakistan is pretty dissimilar as the one that take place all over the world. As contrast with different cybercrimes like hacking, infections, viruses and worms, the most widely victimized and documented cybercrime in Pakistan is online harassment. Online harassing is directed against the females in all respects as often as possible. As indicated by “Federal Investigation Agency's” (FIA) and “National Response Center for Cybercrime” (NR3C), the proportion of 16% of the populace is effectively engaged with the

exercises on the web comprising of web based shopping, web banking, information conversion and correspondence and so on. Nonetheless, access to these innovations and technologies as well are not upsurge to in setting of Pakistan as a result of different elements including; sexual orientation (gender), geographic areas and financial status. Other than that according to the report of Telecommunication (2017), there exists astonishing difference in ratios of men owning the cell phones and ICT as compare to the women in context of Pakistan, thus the ratio indicated that about 84% of the men own cell phone whereas 64% of the female have their own personal cell phone in Pakistan. Consequently the proportion of 75% of the web based clients are male, beside of this fact, still female are more casualties of online and virtual viciousness as contrast to the male (Haque 2013). According to this study, these savagery based enacts contained criticism, unlawful appropriation of individual data, digital harassing and considerably more. As indicated by FIA, out of 3025 recorded cases amid 2015, about 45% has been identified with the online savagery and violence as well as harassment against females.

Foundation (2016) has had a survey on cyber victimization and took a sample of 1400 female for investigation those are the web users as often as possible. It is unveiled by the Foundation, (2016) about 70% of the female has been reveal to have fear regarding their pictures they have posted in couple of years to the social media concerning their harassment and about 40% of the women described that they encountered the state of being annoyed and harassed by message applications (Apps). This study on context of Pakistan revealed the high female cyber victimization. Moreover, as per “Digital Rights Foundation's” (DRF), the cyber harassment helpline, the significant kind of provocation looked by Pakistani females depends on the factors, such as; imitations by 20%, blackmailing by 21%, unwanted messages by 12% and non-understanding information by 19%. Moreover, the two primary reasons of females being

progressively misled through the cybercrimes are; the low adeptness rate alongside less involvement of female in the fields of science and engineering, and the second reason is their family grounds and stereotypes, because of narrow conviction of families they are restricted about the careful conduct and comportment of web which makes these females to feel progressively alluring towards the utilization of web Dad, N. (2016). According to FIA during year 2015 3,000 cases of online harassment against women are reported. On the other side, 45% of these cases were based on the online harassment of women using social media Al-(Jazeera, 2016).

2.6. Restrictions and problems faced by Pakistan concerning Cyber-crimes

Profiles of cyber criminals are different as compared to the conventional criminals. Normally law enforcement agencies do not hold any database which contains all the information about these criminal. This is an important issue which hampers the investigation of cybercrimes mostly. For instance in Russia, most of the cyber criminals are educated and works independently so it is difficult to fit them in one profile of a cybercriminal.

Inefficiency and congestion exists within the law enforcement agencies about the implementation of cyber laws. There are multiple reasons behind it which may include lack of resources, less knowledge and training about the new technologies used by hackers, lack of cross border cooperation and victims unwilling to report the crime (Kshetri, 2006).

Unemployment rate in Pakistan is computed as 6% in 2012-13 which is very high in comparison with other countries. Indeed, even Pakistan generally falls behind of other struggling nations in the list of developing countries. Web turns into a dynamic source to look occupations or win cash in the contemporary condition. The unemployment causes problems at both ends. It

empowers couple of clients to practice ill-conceived strategies to gain financial benefits in most shortest and conceivable time. On the other hand, jobless people may access fraudulent and fake sites for getting better work opportunity. Despite the fact that employed people are likewise vulnerable to the cybercrimes conducted by these websites. In any case, jobless people are normally deceived because of distress caused by the poverty oriented circumstances (A.N. Ghulam Muhammad Kundi, 2014).

The average literacy rate of Pakistan is 79% although Pakistan positioned at 180 among 221 nations in education. The overall lack of education causes numerous issues and cybercrime can be considered one of them. Particularly, people with insufficient internet knowledge and experience are more vulnerable towards the cybercrimes. They can be effortlessly swindled and deceived. Typically such people become victims of money related scams, computer trespassing, spam emails, data stolen frauds, business related frauds and many more. Abecedarian on internet has fascinations. Offenders misuse the necessities of the victims like education, medical cure, and visa and so on because there is less chance of finding the crime source. So normal people can effectively victimized and easily accessible (Sultan Ullah, 2015).

Law enforcement agencies have perpetual issues of less expert manpower. In spite of the fact that transparency is a major concern and considered as the most important aspect featured by any government associations, however the high performing organizations are more vulnerable to the cybercrimes if uncouth human asset are hired. A proactive security measures must be taken, if skillful hiring are made and refreshed after regular time periods.

There is an urgent requirement of cooperation between different governments exists so that cybercrime offenders can be captured effectively across the borders. In any case, the laws are set

up, sanctioned, checked on and refreshed on customary premise in created nations yet immature and creating nations fall behind in such manner. Absolutely, a serious gap exists between various nations to understand the sensitivity of cyber warfare (Y. H. Mujahid, 2002).

In some of the developing nations, cybercrimes are not considered as a genuine concern like violations conferred in the real circumstances. Because of ongoing cybercrime based oppression upshots which were most certainly not conceivable without data exchange through digital means, some of the developing countries have made solid relationship with different nations particularly with Pakistan. The advancement is urging to address the terrorism issues and also the cybercrimes are normal issues of about each domain like advertising, news coverage/broad communications, managing an account and fund, e-government and so on. Government to government participation is mandatory almost for each field (Ghauri, 2014).

According to Pakistani laws there is concrete cyber law to deal with the variation taken place by CII (Critical Information Infrastructure) with less implementation. According to the review of MIT committee, Pakistan requires to implement the cyber-criminal law. Electronic Transaction Ordinance contains only the draft recommendations to deal with the problems related to cyber security. Therefore, it is also highlighted by the committee that there is no specific tool for the security of public and private institutions that can be implemented in order to meet the international standards (Mattoo, 2013).

In digital age, digital security of nation is out of date which is absolutely insufficient and inadequate (Jawad Awan and Shehzad Memon, 2013). When we need to look for Pakistan's National Cyber-Security Arrangement or laws, only two documents exists which states "Electronic Crime/Cyber Bill 2015",which is exhibited twice in National Assembly of Pakistan

for suggestion however it is under survey till now. In spite of the fact, it has therefore changed. At the point when the general population has no access to a perceived, battle and affirmed record at that point it ends up troublesome for common men to help the government official and private associations to achieve CII digital security objectives. Pakistan's Cyber Crime Bill 2007 has been already implemented in the country. But if the overall statistics about the results are studied then the development is zero Awan (J. Awan and S. Memon, 2016).

Accessible crime equity legitimate system in Pakistan is not adequate and is not capable to discourse the contemporary threats created by cybercrime. This new age impeded both existing crimes when steered with the web practices and has carried out new dimensions of crime and especially cybercrimes. These advanced cybercrimes cannot be dealt viably with the usage of already existing legitimization. These new kind of violations require totally new and extensive laws that should concentrate on the online activities of people and organizations. Besides, it is seen that 800 million information records from developing nations have been already hacked. In such conditions, third world countries for example, Pakistan need to prescribe approaches to control the cybercrime warfare in close cooperation with other developing countries (Mirza, 2013).

Basic safeguard measures for vital digital administrations of the nation; NADRA (National Database and Registration Authority), E-Government administrations and capital showcases likewise requires consideration of government in current security circumstance. These organizations are utilizing firewalls and other advancements to secure frameworks, but still there are numerous conceivable outcomes by which the cyber criminals can utilize more advance

technologies as a source to assault, control and stop the basic ICT administrations in Pakistan (Pakistani, 2013).

Currently, Pakistan has no ultimate law to comprehensively deal with the prevention of those measures creating danger of cyber-crimes. Pre-existing laws within state in this regards are inadequate and not solid and steady to direct the cutting edge cyber-crime threats of advanced era. This modern era incapacitated in cooperation with the existing infringement when coordinated with the use of web and has delivered another kind of cybercrime space, for instance, hacking (Unlawful access of data), impedance with data and ICT structures, extraordinarily advanced rerated electronic imitation and cheats, computerized attacks on fundamental ICT establishments, unapproved square endeavor conveyed by regular citizens, Identity theft and utilization of malignant code to watch out for ICT systems. These cybercrimes can't deal feasibly with or repelled utilizing effectively existing laws. These remarkable crimes require an absolutely new and exhaustive legal act that will focus on the online lead of individuals/affiliations (Holt, 2012). According to Usman, M. (2016), Pakistan is facing immense internet complexity to cope with the cyber victimization. The approachability of computers and the web associations have made much easier to communicate, interact and to be educated by getting knowledge via web within state. Notwithstanding, certain folks (and companies) do misuse the intensity of the Internet for criminal purposes. According to this study, First historically dialogue enactment Pakistan has in arena is "Electronic Transactions Ordinance, 2002", addressing the cybercrimes matters, additional to this the Ordinance was proclaimed by the President of the Pakistan with the goal "to perceive and encourage reports, records, data, correspondences and exchanges in electronic structure, and to accommodate the accreditation of confirmation administration providers." However, this does not talk about the

entire situation of web and computer misconducts and offences. Scarcely any things are secured under this law. Then there is another significant enactment in Pakistan's legitimate framework. This was, “the Prevention of Electronic Crimes Ordinance 2007”. It was proclaimed to give attention to online wrongdoings (Usman, M., 2016). This ordinance thus declared thrice within state; at first in May 2008 and then in February 2009, however, the last declaration of Prevention of “Electronic Crimes Ordinance” occurred on fourth July 2009. This ordinance was claimed as presidential ordinance and practices fir 120 days from its date of declaration. These facts reveal that there was no any specific long lasting and strictly practicing law to prohibit the digital violence in Pakistan. Thus, it is unimaginable to expect to take out digital wrongdoing from the internet completely from Pakistan or from the world. In any case, it is very conceivable to check it and take sudden actions to decrease it by making mindfulness among the clients of the web. The indispensable improvement is to make individuals mindful of their rights and obligations and further making the utilization of the laws progressively stringent to check wrongdoing and cyber-crimes to prevent and get rid of this problem (Mohiuddin, 2015).

The current practicing act in Pakistan is “Prevention of Electronic Crime Act, 2016”, although the act is quite comprehensive as compared to the previous legitimate acts but does not cover all of the criminal practiced domains of cybercrime active in Pakistan and again it is more in paper as compare to in practices (Usman, M., 2016). It is revealed from the dawn report presented by Qarar, S. (2018), on statistics of FIA, cybercrime has been hit the record in 2018, as the harassment and blackmailing cases concerning the women has been sharply increasing from past three years, according to FIA cybercrime cell has so far led 2,295 request, enrolled 255 cases and made 209 captures in 2018. The relating figures for 2017 were 1,290 request, 207 cases enlisted and 160 captures made, though figures for 2016 remained at 514, 47 and 49. The FIA conceded

that cybercrimes are on the ascent in Pakistan yet included that "the administration's ongoing measure to build up 15 new cybercrime notifying centers" will help control the circumstance (Qarar, S. 2018).

As indicated by (APWG 2013) cyber hackers have attempted to get to the data identified with the exceedingly touchy government associations primarily military. These kinds of assaults are made conceivable by utilizing DDOS. Anyway FIA can't stop these assaults due to less skill in this area (Jawad Awan and Shehzad Memon, 2013). There are various terrorist associations and unidentified groups over the globe. They have increasingly citified innovation and very much prepared individuals in the field of cybercrimes. These individuals are filling in as an individual or as a group. Upon these groups there are not many which are working freely and any sort of law can be invigorated on them on the grounds that to discover them clairvoyantly is likewise a noteworthy resistance. That is the reason these groups of secretive individuals are making an unwonted dangerous situation for the national security of Pakistan. Pakistan's computerized structure isn't successful so as to perform counter assault and to stop the unlawful access to the private information. Also numerous psychological militant associations are physically present in Pakistan so it is considerably more difficult circumstance for the general security of Pakistan.

Common people don't have consciousness and awareness concerning the digital laws that as of now exists. Likewise they don't know about how to shield their very own data from hacking or unlawful access because of which they become the casualty of cybercrime. The financial organizations such as banks in Pakistan are expanding their reliance on the internet. In any case, alongside this online extortion and robbery of charge card information is likewise expanding which is a genuine danger to the Pakistani consider. Because of this reality common man is losing its trust on the banking system.

According to (Masud Ahmed Malik, 2018) the reasons for cybercrimes in Pakistan are as follows:

- There is no awareness about the importance of security measures about the cybercrimes both at organizational and individual level.
- Highly qualified and trained man power in domain of cybercrime preventive measures is not available.
- There is no policy about the email accounts of people from security agencies, police and armed forces. Cyber-attacks are not only coming across the globe but the major threats we have are from our neighboring countries.
- The minimum eligibility to join the law enforcement or police agencies does not include any knowledge of computers so most of the people have no knowledge about the new technologies in cybercrime.
- The progress of government is quite slow in comparison to the speed of technology advancements in cyber technology. Therefore government is not able to determine the origin of these cybercrimes.
- Research & Development and promotion in latest technologies especially ICT is not according to latest standards.
- Law enforcement and security personnel are not equipped with technology to address high-tech and complex crimes.
- Present governmental policies are not self-governing so that cybercrime across the borders can be investigated effectively.

- Economic budgets for security objectives by the government especially for the training of law enforcement, security personnel's and investigators in ICT is quite low as compare to other countries.

On concluding remarks it is thus outlined that, there is no comprehensive investigation has been found in contextual studies concerning the gender based cyber victimization. Cybercrime is the most talked about issue in today's world problems. The victims of the cyber-crimes are not the residents of one specific state or country, rather the issue is common within all states and has been discussed by many of the researchers. Generally there are such huge numbers of concentrates in setting of United Kingdom, Europe and United States of America. The ratio that how many women victims have been victim of cybercrime is not exact. Likewise how the Pakistan is managing cybercrime issues is a central issue mark for the world. People in Pakistan reported to be more prone to be cyber victimized due to their unawareness of the cyber-crimes and the laws as well. Moreover the practicing of the cyber-crime prevention laws is not satisfactory within state as reported by the literature. So, these gaps of unawareness, non-categorization of gender and age of the victims to propose a specific victim bases policy, and the non-addressed causes of the occurrence of the cybercrime along with the best optimal solutions would be filled out with this research study. Moreover, this investigation will give an exhaustive review of the exploited people in cybercrime and furthermore will talk about the distinctive preventive estimates that have officially taken for halting the cybercrimes.

Chapter 3

Methodology

3.1. Introduction:

As discussed in the opening chapter that the key objective of the study is to examine the "Cybercrime in Pakistan: detection and punishment mechanism". In order to meet the objectives of the study this chapter presents methodology undertake and justify the problem statement. Research methodology is an overall plan stipulating the rationality of the theory development process and an applied framework to conduct research (Remenyi et al., 1998), therefore, according to Mohajan, H. (2017), research methodology provides the criterions to organizing, arranging, structuring, and leading the research and the methodological choices those are uttered by the research paradigm followed by a researcher. There is a difference between research methodology and research methods has been pointed out by the contextual studies, as Giddings, L.S. (2006), stated that research methodology is related to the tactics adopted by the researcher through bordering the research interrogations and procedures, on the other hand the manner in which the data is gathered and analyzed for research tenacities is known as research methods. Bhattacharyya (2006), had presented the similar concept and articulated that the research methodology is quite wider in scope as compare to the research methods, as the research methodology is a holistic phenomenon comprised of research methods, the philosophy of choosing the particular research techniques and the procedures of determining the results of research with the particular methods. Thus to fulfill the definition of the research methodology this chapter covers the overall methodological grounds of the research including; research

paradigm, research approach, research design (population, sample size, sampling techniques, research variables), the tools of data collection and ethical considerations.

3.2. Research Paradigm:

Vosloo, (2014) argued that, paradigms are the cardinal part of social sciences research, as it holds major impact on methodology and philosophy of the social science. According to Neuman (2013) and Blumberg et al. (2014), it is a holistic structure of intellectualization and belief explaining how the research would be conducted; coherent and observed is known as research paradigm. In more specific connotations, paradigm is the description of the philosophical assumption associated with the nature of social reality (ontology-the believe about the nature of reality), the way to know the reality (epistemology-how do we know what is known to us), ethics and value system associated with research (axiology-the believe about the truth), appropriate approach of the inquiry (methodology-how should we conduct the research) (Patton, 2002). There are three main schools of thoughts associated with the paradigms; Positivism, Interpretivism and Pragmatism (Chilisa, 2011), along with two cores thoughtful assumptions know as ontology (The concept of knowledge) and epistemology (the acquaintance of knowledge). Whereas, the other assumptions related to the paradigm are the axiology (the principles of research), rhetoric (the writing techniques) and methodology (the procedure of the research) (Creswell 1994).

Table 3.1: Basic Research Paradigms

Paradigm	Ontology	Epistemology	Methods
Positivism	Hidden instructions administer teaching and learning process	Consider the reliable and valid tools to uncover the directions	Quantitative
Interpretivism	Reality is created by individuals in groups	Discover the underlying meanings of the events and activities	Qualitative
Pragmatism	Truth is somewhat which is useful	The best method is one which present the solution of the problem	Mix-methods Design-based

Source: Saunders, M. Lewis, P. and Thornhill, A. (2009).

The positivism paradigm follows the single objective reality of the research (Hudson 1998) and is linked with the quantitative approach of the investigation. The positivists follow operational approach of research having a clear topic of research, hypothesis and the appropriate methodology to testify those hypothesis (Churchill et al., 1996), then mathematical and statistical techniques operated to generate the object and reality based results (Carson, 2001). The

interpretivism on the other hand is the approach of the research believing that the reality is multi layered and is associated with the rich human interaction (Pring, 2000), and follows the qualitative approach of research. The inspiration driving examination in interpretivism is sharpness and interpreting conventional activities (events), experiences and social structures, similarly as the characteristics Collis & Hussey (2009) and Rubin & Babbie (2010), people's attach to these wonders, interpretivists thus, believe that social truth is passionate and nuanced, in light of the way that it is formed by the perspective of the individuals, similarly as the characteristics and purposes of the researchers. And finally the third concept of the paradigm is pragmatism which is the combination of upper mentioned both of the approaches and also known as mix-method approach, because it enjoy the attributes of both of the researches and is quite wider and detailed as compare to prior mentioned approaches (Tashakkori and Teddlie, 1998).

As this research study is mainly about to investigate the victimization in the domain of cybercrime in context of Pakistan through the quantitative measures, hence follows the 'positivism' paradigm. This research study possessed all characteristics of the objective reality. Hence, we will explain the paradigm of positivism. Positivism paradigm is further explained with two most important philosophical assumptions with respect to explanatory research namely Ontology and Epistemology.

- **Ontology:** Commonly known as knowledge representing the area of information with respect to nature of reality, specification of constructs and body of knowledge is ontology **(**Jfermiller, 2010).

The ontological view of the current research study explains that there exists only one reality of the nature, thus the investigation of the hypothesis to address the gender victimization in domain

of the cybercrime would be tested with the properties of positivism which is external to reality as well.

- **Epistemology:** Epistemology is empirical in nature and narrates the method of adopting knowledge, for example it discusses how the knowledge is acquired and its acceptability (Blumberg, et al., 2008).

Epistemology is concerned with the knowledge acquiring for a particular research problem. It involves the methods of the data gathering and its utilization. For this current study of positivism it is explained the data would be gathered here with and through well designed questionnaire based on self-made scales of measurement associated to the research problem.

3.3. Research Approach:

The research approach generally is could be of two types; either deductive or inductive research approach (Saunder et al., 2009). Another approach which is emerged with the blend of the deductive and inductive approach is known as mix method or blended approach in literature (Greene and Azevedo, 2007). The deductive research approach is purely associated with the positivism paradigm in which testing of hypothesis based on cause and effect relationship among the constructs of the study and is highly structured in nature, on the other hand the inductive approach is one which is linked with the interpretivism research paradigm and is quite flexible in order to generate the results and follows the observations and human interactions for generating the results. Howsoever, the mix method approach is the combination of the two aforementioned approaches. Because, positivism paradigm is used with quantitative approach which is most suitable approach of data collection and statistical analysis, the quantitative deductive approach which is empirical in nature is more appropriate to use for this current investigation about the

gender victimization in domain of cybercrime within context of Pakistan. In this research deductive approach is used to empirically test the propositions. To accomplish this objective a theoretical framework on the basis of supporting literature was developed and the relationships proposed in this framework has been articulated by using the quantitative research techniques for sake of testation of the hypotheses.

3.4. Research Design:

Research design is a comprehensive plan to follow the taxonomies of the research; hence research design lay down the overall foundation of the procedure to conduct research and data collection (Leedy, 1997). Leedy and Ormrod (2005) explicated that, there are three basic research designs found in literature; descriptive research design, exploratory research design and the explanatory research design, whereas the descriptive research design is used to give comprehensive description of the issue addressed in the research investigation object as they encountered, the exploratory research design is about to investigate the new things those are not investigated before and the final one the explanatory research design is one which is linked with the explanation of the cause and effect relationship among the selected constructs of a research investigation. This research study is about to investigate the cybercrime victimization in context of Pakistan, thus is exploratory in nature to reveal the "Cybercrime in Pakistan: Detection and Punishment Mechanism".

3.4.1. Justification for Selected Group of Students

The considered group of population for the current research is students from the 30 top ranked and high enrollment rate universities of Pakistan. 400 students have been surveyed for this concern. Whereas the high ranking and high enrollment has been ensured through the HEC

ranking list. The students have been considered as the targeted population because, most of the time they are online through different social media websites and there are more chances that they are being victims of cybercrimes. Basically, the selection of this group of students is its appropriateness with presented theoretical context of the study. Therefore it is an effective way to discover the reality specifically from people who are viewed as the most important part of online revolution. The following reasons may explain the selection of the students as a sample. First, the students are more web users as they have to use the internet for educational purposes and for getting updated knowledge about the world. Secondly, this group of people is more active in using social sites and has confidence of interaction with anybody via using internet. These facts make them higher in cyber victimization. Thus, the most suitable population for this study is the university students.

3.4.2. Sample and Sampling Technique:

Sampling technique varies with research objectives and subject matters accordingly. However, generally there are two main sampling techniques for data collection; probability and non-probability sampling (Saunder et al., 2009). Although, the probability sampling ensures the equal chances of all respondents to be selected for survey, and in non-probability sampling there are not equal chances of all of the respondents to be the part of investigation from population (Alvi M. H., 2016).

This research study utilized a non-probability sampling technique. Here, rather than the researcher choosing respondents, there was a self-selection performed by each respondent itself. Therefor the decision to participate in a questionnaire is done by respondent itself. The reason of selecting non probability sampling technique lied in a fact that the population is quite large and precise number of population is unknown , there are many studies in literature using non-

probability sampling technique for quantitative studies when the population size is unknown (Alvi, M. H., 2016). The volunteer or self-selection sampling technique is further utilized here because of its appropriateness with the problem statement and the targeted respondents as this sampling technique is based upon willingness and interest of the targeted population to be the part of the study to provide the precise information (Costigan and Cox, 2001; Abrams 2010). Thus, to enhance the sampling results in a better manner, the researcher has used the self-selection non probability sampling technique. Other than that the researcher tried to promote the research topic through different online medias i.e. social websites, e-mails, direct messaging etc. Therefore, since respondents choose themselves, it was most certainly not doable to utilize the concept of equal probability of selection technique as used for probability sampling.

3.4.3. Sample Size

To draw the sample size a sampling frame is used, whereas sampling frame contains the list of targeted population. The top ranked universities of Pakistan with high enrollment rate has been selected to determine the sampling frame of this study. The reason of targeting these universities is that these universities have more educational departments and thus have more students as compare to other universities, thus it is easy to gather the required sample of the study from the genuine respondents. In this context 30 universities have been targeted and 400 students have surveyed. Moreover, the sample size of 400 also satisfied the requirement of sample size for online survey, as per Krejcie and Morgan (1970) formula 285 responses are sufficient for quantitative study and for unknown population when the propositions are tested on the bases of population proportion expressed as 0.5 (50%) with 95 % confidence of internal and margin of error at 5% (0.05).

Sample Selection Formula:

$$"n = \frac{N}{1 + Ne^2}"$$

Where:

"n = Sample Size

N= Population

e= α= 0.05 (5%)"

Thus 400 is an adequate and sufficient sample size for quantitative research study.

3.5. Data Collection and Instrumentation:

After selection of the research design, sampling technique and sample size the data collection and the instrumentation is the next step in a research. Data collection is the critical part of the research as the results and the worth of the research relies upon the collected data. That's why the procedure of data gathering and instrumentation must be appropriate to have reliable and accurate results of a research study.

3.5.1. Instrument and Technique:

Saunder and Lewis (2012); Collis and Hussey (2009) discussed that quantitative research involves two types of techniques for research. The one is survey technique and the other is experimental technique. The survey technique further categorizes in two forms; the structured interviews and the self-completion questionnaires with or without the presence of interviewer. Some research studies used mono-techniques while other uses multiple methods for research

dedications. This study based upon the survey method in order to collect the data from the top ranked and high enrollment rate universities of Pakistan. This survey approach accumulates important, explorative and vital information from the target group of population. The data collected from this approach is quantitative in nature and the results would be derived from the analysis of online research content and additionally from a dataset generated by responses of the targeted population. Along these lines, the review questions would be detailed in light of the subjects emerging from the observational writing on the field, the student's feedback and my hypothetical analysis. Analysis of questionnaire results also enables the research to be more accurate (Creswell, 2017)**.**

The online survey method is considered to be best suited for this study because of certain reasons which are based on certain factors. Above all, the presented research question is an exploratory one and survey method is presumed as a viable procedure for collecting the exploratory information. Subsequently, considering the fact that the number of participating group is bigger, this methodology offers logic and competence and helps to connecting with a huge extent of the objective population effectively and the targeted population is considered to be more active at web and internet use. Also in previous research of criminology so many people have used survey methodology in order to reach to the logical and valuable results (Yang, 2006).

In order to collect the primary data from the group of respondent's research tool based on the questionnaires designed by researcher has been used concerning cybercrime and cyber victimization to add authenticity in the results.

3.5.2. Questionnaire and its Instrumentation:

The well designed questionnaires will be used for collecting the data from the university students. The questionnaire method is better than face to face interview method because of numerous reasons. The first reason is that the students are not able to give face to face interviews because of embracement they feel while discussing their personal information openly. Second reason is that the questionnaire method is short and gives more insight about the respondent. The "online surveying" methodology is opt to consider as research tool of this study as it overcome the above mentioned problems and the time as well as geographic constraint are thought to minimize with online survey to increase the potential participants of the study (Andrews, D. et al., 2007). The questionnaire comprise of both open and close ended questions.

3.5.2.1. Reliability and Validity of Questionnaire:

The reliability and the validity are critical for any of the research study and it is measured through the scale or items of investigation of specific constructs. To ensure the reliability and validity of the responses is checked through Cronbach's coefficient of alpha having value above than 0.7 (Hair et al. 2010). The basic tool for collecting primary data for this research is based on the questionnaires. The earlier draft of questionnaires is tested with 20 students and on the basis of their feedback further modifications are made. These modifications were based on the changing the explanation of questions and making them simple so that normal student can easily perceive it. The questionnaire is self-developed because there are very few studies in literature following the quantitative techniques of cybercrime and their existing measures do not possess the suitability of them to be practiced on domain of Pakistan, as the culture, internet using trends and the victimization scenarios are quite different in Pakistan as compare to the other nations. **Pilot Testing:** Pilot study is the small study test regarding the research protocol, techniques,

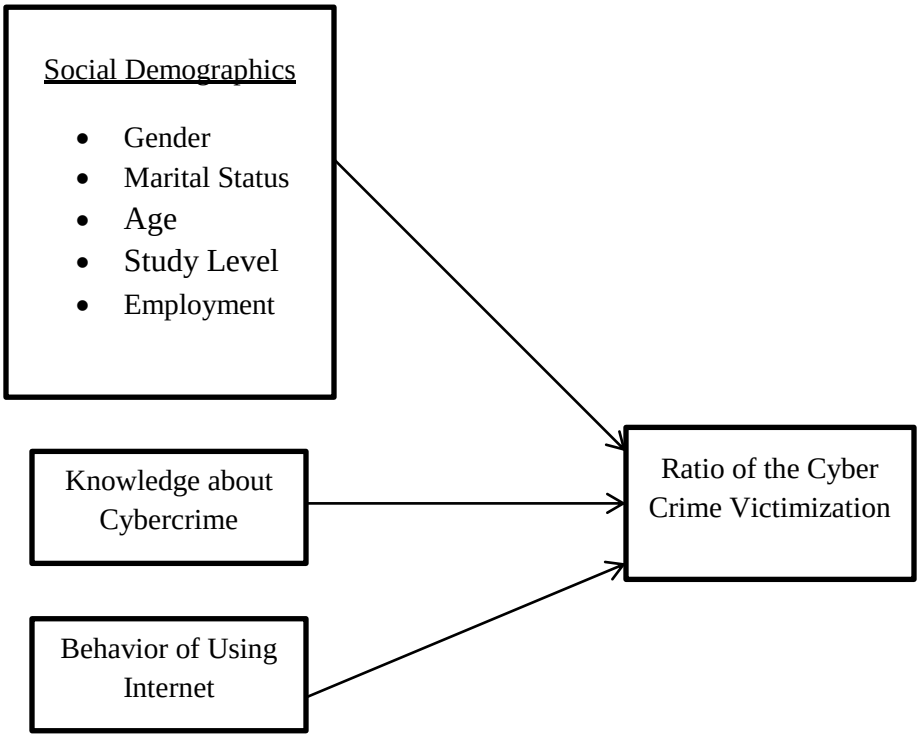
instruments, sample recruitment strategies and other research techniques before applying the particular research to the larger study (Hassan et al. 2006). The prior tested 20 questionnaires have been gone through the pilot testing as well. Thus to confirm the reliability and validity of the research instrument and to overcome the deficiency at early stages, the researcher practiced pilot testing with and through the self-developed questionnaire determining the "Cybercrime in Pakistan: Detection and Punishment Mechanism". The understanding of statement to the respondents has been ensured by getting responses on initial questionnaires and then the responses were added and calculated in dummy tables. The internal consistency of the items was ensured at this stage with the cronbatch's coefficient greater than 0.7 for each of the item investigated. After the procedure of the pilot testing the actual data collection was practiced.

3.6. Theoretical Background:

This study is based upon the phenomenon of "Cybercrime in Pakistan: Detection and Punishment Mechanism", thus "Routine Activity Theory" is the base theory of study. This theory has been proposed by Cohen and Felson (1979) and presents the concept of crime occurrence by having three core components of crime manifestation; availability of appropriate target, a driven offender or criminal and non-availability of proficient guardian to prevent the incidence of criminal act. The founders of this theory (RAT) considered that analyzing how and why criminal offenses happen in certain places and circumstances might be helpful and imperative to an investigation of cybercrime victimization (Jahankhani, H., 2013). This contention depends on the idea that cybercriminals regularly look for reasonable and significant focuses in explicit sorts of social fields (Piazza, 2006).

3.7. Analytical Framework:

Figure 3.1: Analytical Framework



Source: Authors' own designed framework

3.8. Hypotheses:

H_1: The knowledge about the Cyber-Crime is not important

H_2: Ratio of women is higher as compared to men in case of cybercrime victimization

H_3: Students spending more time on internet have more risk to become a victim.

H_4: Chances of sexual harassment and cyber bullying increased by only using social media or online other online resources

H_5: There is a significant relationship between socio-demographic factors and cybercrime victimization

3.9. Variables:

The above presented analytical model represents the effect of independent variables (IV's) on dependent variables (DV's) (see figure 3.1). The independent variables has been selected on the basis of proposed research, Independent Variables consist of the knowledge about the types of cybercrimes, socio-demographic feature, amount of time, already existing experience. The basic idea of this implementation is to apply these variables in the context of cybercrime effectively. The variables and responses of the questionnaires are coded in SPSS to generate the statistical results.

Dependent Variables

Ratio of cybercrime victimization: This variable is representing the proportion or percentage of the cybercrime victimized.

Independent Variables

I. **Social Demographical statistics –** age, gender, marital status, study level, employment, family income
II. **Knowledge about Cybercrime**
III. **Behavior of using Internet:**
IV. **Other Controlled Variables**

For the clarity of results few other variables are also considered which are connected to basic variables already defined. These variables generally stated as demographic profile of respondents.

- Location of Residence
- Study Level
- Age
- Income
- Marital status

Other than these variables, a demographic "name of your institute" has been added to the questionnaire in order to make sure the responses has been generated from the targeted desired universities (See Annex-1).

3.10. Data Analysis and Analytical Model:

The data has been analyzed through SPSS and findings are explicated in form of; Descriptive Statistics, Frequency Distribution and Reliability Analysis.

- In data analysis different graphical charts and bivariate tables has been presented to show and evaluate the results for each of the construct of the study on collected data.
- In order to present and analyzed the effect of independent variable on dependent variables regression analysis has been carried out with and through statistical operations on data. The verification of the proposed hypotheses has been presented with regression analysis by having significance level i.e. p-value ≤ 0.05.

3.11. Ethical Consideration:

All research activities accompany different moral and ethical issues. This research is also not unique and raised important ethical issues as well. The moral issues included encapsulated the three integral and commonly strengthening standards including respect for people, concern about

their welfare and equity. Therefore all the results that come from the current research are addressed to be kept confidential in order to save the integrity and respect of questioned group. For each participant the questionnaires have been sent through email, social sites and direct messaging as well. So that all those participants who do not want to give face to face replies of questions can easily fill them online. This approach helps in protecting the confidentiality of participants.

Chapter 4

Results and Interpretations

4.1. Introduction:

This chapter presents the findings and their interpretations.

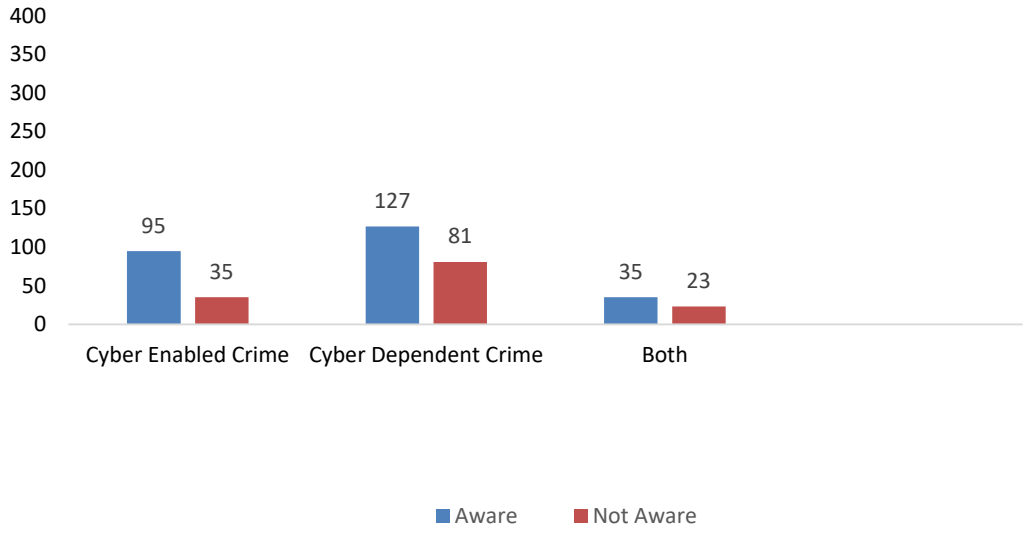
4.2. Descriptive Analysis:

Descriptive analysis involves numbers in it to summarize the data with an intention to describe the particular results (J. Toby, 2016). Primarily descriptive analysis focuses on detection of sample characteristics those greatly influence the conclusion of the study (Thompson, C. B. 2009). Here in analysis of current research study, descriptive analysis involves the representation and interpretation of the results in forms of bar charts to present the statistical outcome of the responses as given below:

4.2.1. Awareness about cybercrime:

The data has been collected on awareness about the cybercrime among the university students in domains of “cyber enabled crime” and “cyber dependent crime”. The results have been presented in form of bar chart given below (see Figure 4.1).

Figure 4.1: Awareness about Cybercrime



Total 400 responses have been made, out of them 4 have not answer about awareness thus, and 396 actual responses have been gathered. In concern of awareness about cyber enabled crime 95 out of 400 respondents' i.e. 23.75% said that they are just aware about cyber enabled crimes, 35 respondents out of 400 i.e. 8.75% reported that they are not aware of cyber enabled crimes. On the other hand in concern of cyber dependent crimes 127 respondents out of 400 i.e. 31.75% said that they are just aware about the cyber dependent crime and 81 respondents out of 400 i.e. 20.25% said that they are not aware about cyber dependent crime. And in terms of the awareness of the both kinds of the crimes 35 out of 400 respondents i.e. 8.75% said that they have awareness of both kinds of cyber-crimes but 23 out of 400 respondents' i.e. 5.75% reported that they are neither aware about cyber enabled crimes nor cyber dependent crimes (see Figure 4.1). The presented ratios depict that the awareness about the terminologies of the cybercrime among university students is quite low.

4.2.2. Socio Demographic Factors and cybercrime victimization

There are multiple socio demographic factors those have been tested for cybercrime victimization i.e. gender, study level, employment, marital status, location, reporting to the law enforcement agencies and usage of security software. Each of the factors has been analyzed and presented separately in blow given sections.

4.2.2.1. Gender and Cybercrime Victimization:

400 responses have been collected for gender based cybercrime victimization. The results have been presented in form of bar chart (see Figure 4.2).

Figure 4.2: Gender and Cybercrime Victimization

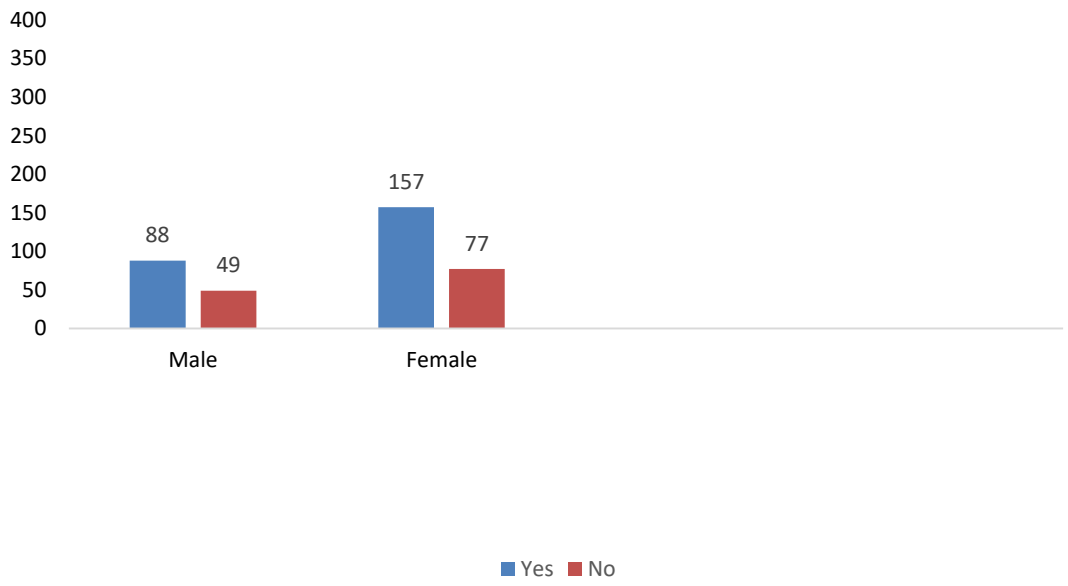


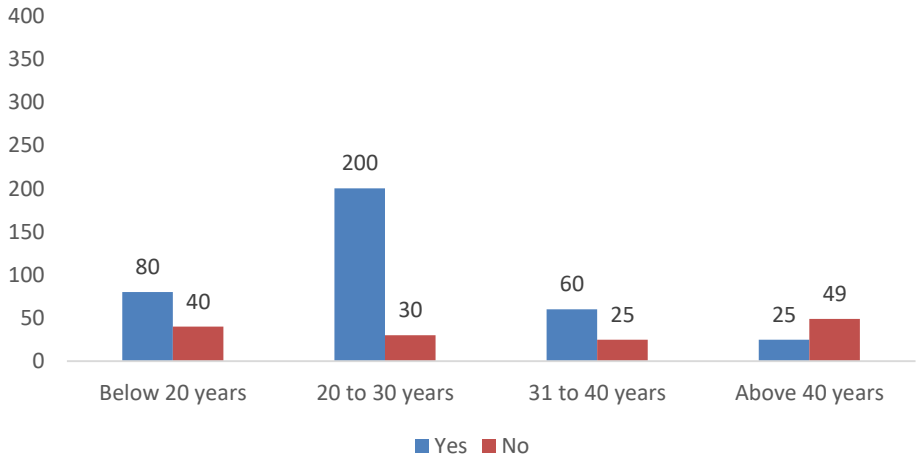
Figure 4.2 presents the responses on ratio of cybercrime victimization on basis of gender. The data have been collected in response of the cybercrime victimization in past six months. It is here revealed that among 400 respondents 88 male respondents i.e. 22% are those reported that they

have been victimized of cybercrime and 49 male respondents' i.e. 12.25% said that they have not been victimized of cybercrime. On the other hand in concern of the female respondents 157 female out of 400 respondents i.e. 39.25% said that they have been victimized of the cybercrime and 77 female respondents out of 400 i.e. 19.25% reported that they have not been victimized of cybercrimes. On collective basis 61.25% respondent have been reported to be victimized by cybercrime by having greater ratio of the female victimization (see Figure 4.2)

4.2.2.2. Age and Cybercrime Victimization

400 respondents were targeted to investigate the ages and cybercrime victimization among university students. Four segments of the ages have been created on average age basis of the students from Bachelors levels to Doctoral degree programs; below 20 years, 20 to 30 years, 31 to 40 years and above 40 years (See Figure 4.3).

Figure 4.3: Age and Cybercrime Victimization



In concern of the age and cybercrime victimization 365 people have given response. The results show that the students who are below age of 20 years reported that 80 out of 400 i.e. 20% have been victims of the cybercrime, the 200 respondents out of 400 i.e. 50% having ages between 20 to 30 years said that they have been victimized of the cybercrime, 60 respondents out of 400 i.e. 15% having ages between 31 to 40 years reported that they have been victimized of cybercrime and 25 out of 400 respondents i.e. 6.25% said that they have been victimized of the cybercrime (See Figure 4.3). The results reveal that the highly victimized age group by cybercrime having ages between 20 to 30 years.

4.2.2.3. Study level and Cybercrime Victimization

Study level of the respondents has been investigated in terms of full time or part time study. The data has been collected with consideration of past six months. The effect of study level with respect to cybercrime victimization has been tested to evaluate either the respondents engaged in full time study are more victimized or those engaged with part time studies. The results have been presented below in bar chart form (see Figure 4.4).

Figure 4.4: Study Level and Cybercrime Victimization

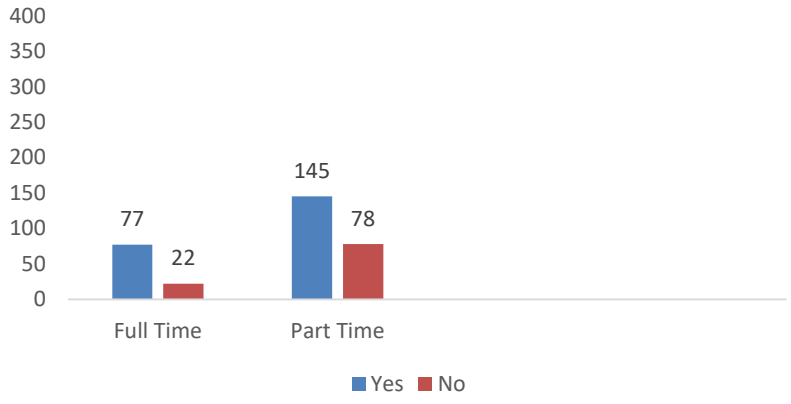


Figure 4.4 represents relationship between the study level and fear of cybercrime victimization. The results show that the students who are engaged in full time study level are 77 respondents out of 400 i.e. 19.25% think that they are vulnerable to become a cyber-victim and they are facing cybercrimes. On the other hand in case of part time students 145 respondents out of 400 i.e. 36.25% feel that they have faced cybercrime. The ratio of the cybercrime victimization in of the respondents engaged in part time study level is higher as compare to the full time students. The reason of the difference in ratio falls in fact that the full time students may not find extra time to be engaged with social interaction and use of internet other than educational purposes while the part time students may be more social via internet and use the web for entertainment or other time spending activities.

4.2.2.4. Employment and Cybercrime Victimization

The nature of employment status with respect to the cybercrime victimization has been tested and results have been presented in below figure 4.5 in terms of bar chart. Here those students have been evaluated engaged with the study and job on shift basis. The respondents have demonstrated the responses by focusing on the activities of past six months.

Figure 4.5: Employment and Cybercrime Victimization

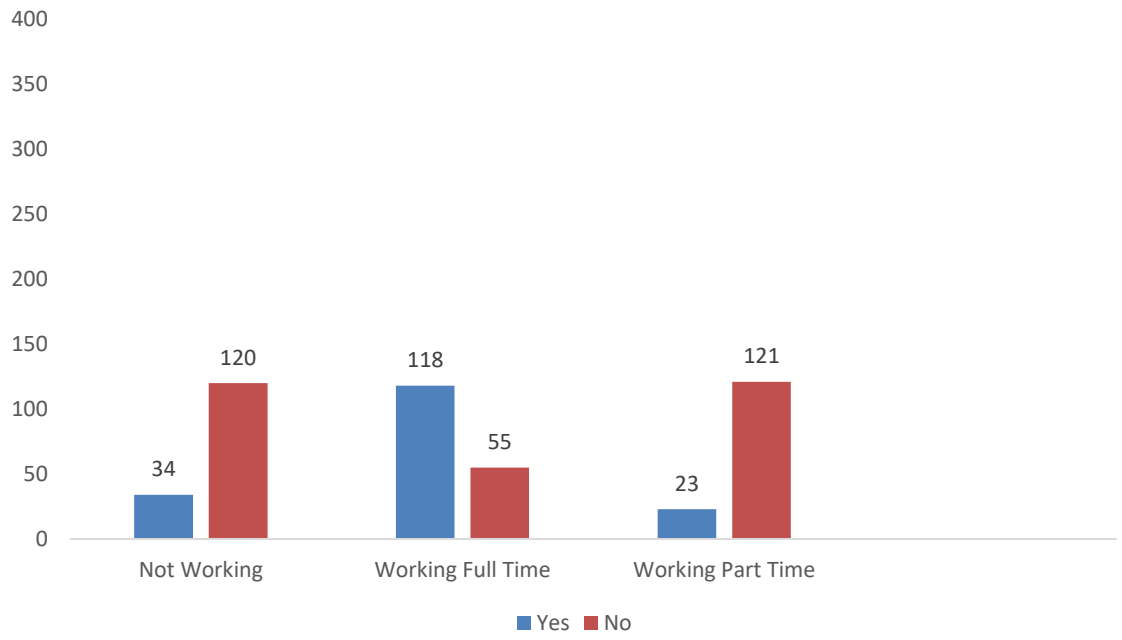


Figure 4.5 shows relationship between the employment status and cybercrime victimization. The results show that the students who are not working i.e. 34 out of 400 respondents (8.5%) or working part time i.e. 23 out of 400 respondents (5.75%) have faced less cybercrimes. These respondents think that they are vulnerable to become a cyber-victim and have faced few cybercrimes like hacking and spam emails. In case of students who are working full time i.e. 118 out of 400 respondents (29.5%) said that they feel they are facing different cybercrimes. According to them being at job and study simultaneously they have to engage with multiple activities via web or internet. So, they have encountered many cases of being victimized during past six months.

4.2.2.5. Marital Status and Cybercrime Victimization

The effect of marital status on cybercrime victimization has been tested as one of the socio demographic factor of the study. 400 responses have been collected in this regards. The marital status has been categorized as; single, married, divorced and widow to determine which category is being more victimized by cybercrime of have higher fear of it. For this study, the students have not been targeted on basis of specific programs i.e. Bachelors, Masters and Doctoral degree programs rather all of them are the potential respondents of the study, by considering this point the sections of the divorced and widow have been generated. The results have been presented in form of bar chart (see Figure 4.6).

Figure 4.6: Marital Status and Cybercrime Victimization

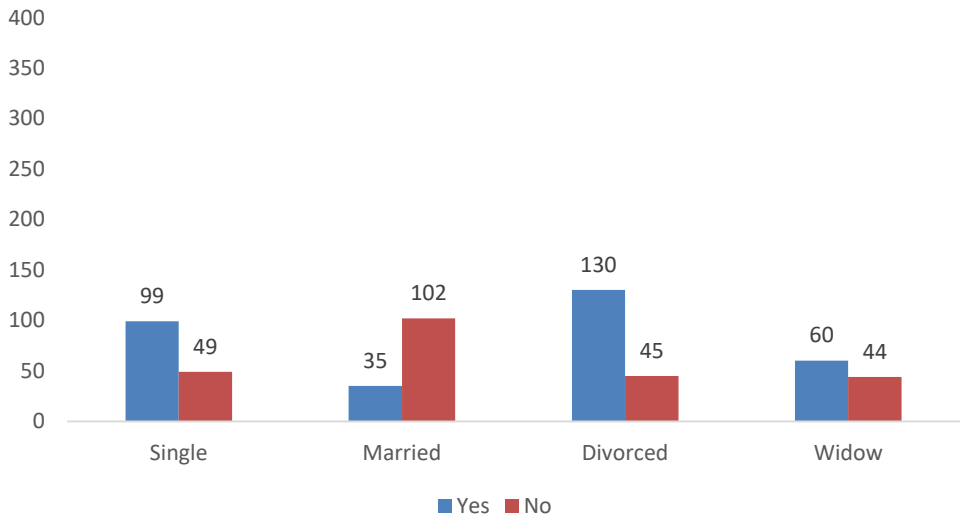


Figure 4.6 shows the relationship between the marital status and fear of cybercrime victimization. The results show the ratios; 99 out of 400 respondents (24.75%) are those single people responded positively about the fact that they have faced cybercrime in different forms, 35

married respondents out of 400 (8.75%) thinks that they have faced a cybercrime in last six months, 130 out of 400 (32.5%) respondents are divorced reveals that they have become a victim of cybercrime in terms of online harassment or bullying from their ex-life partner as well and in case of widow 60 out of 400 respondents (15%) said that they have faced different kinds of cybercrime in last six months. These percentages and figures reveals that the divorced respondents are more victimized, the single respondents place at second position at being victimized via cybercrime, married respondents are at third level in this regards and widow are lesser as compare to other categories of being cybercrime victimized over the last six months.

4.2.2.6. Location and Cybercrime Victimization

The residence of the respondents i.e. location of their living is also being tested in an association with cybercrime victimization from the targeted respondent on domains of; on the campus residence, off the campus within city and off the campus in rural areas. The reason of these categories for survey is lies in the fact that those residents within institute campuses could not access each of the website and social site due to certain proxies on institutional internet, those living at off the campus but within city have more opportunities to access the internet as compared to other two categories and those living at off the campus but in rural areas might have troubles of signals and other services issues in accessing the internet. 400 active responses generated who had responded about their residence at; on campus, off campus in city or off campus in rural areas. The results have been presented in form of bar chart (see Figure 4.7).

Figure 4.7: Location and Cybercrime Victimization

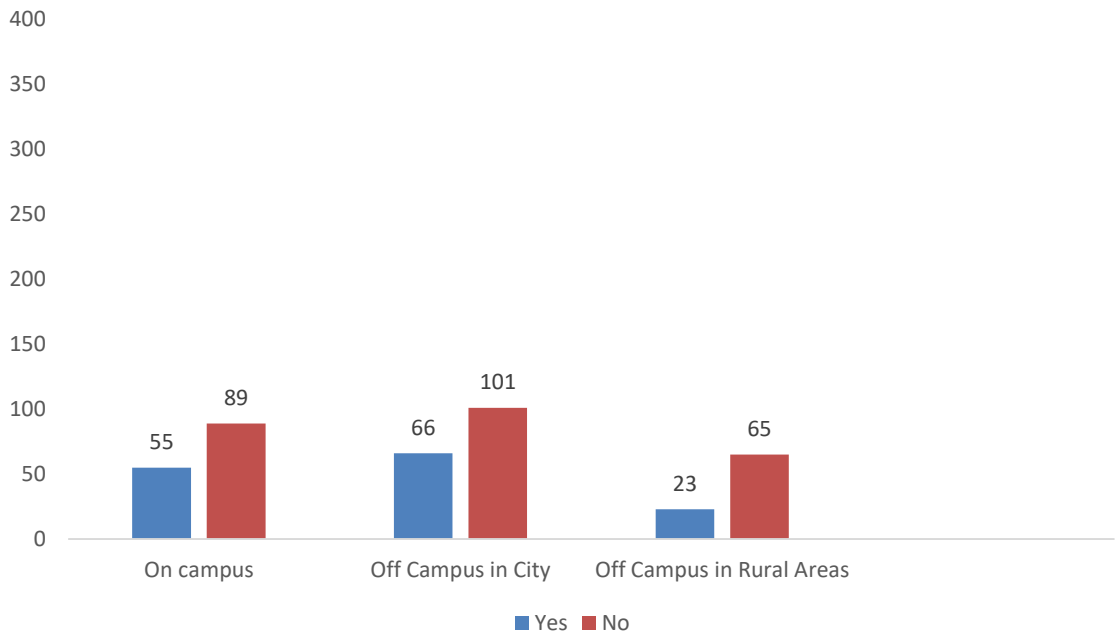


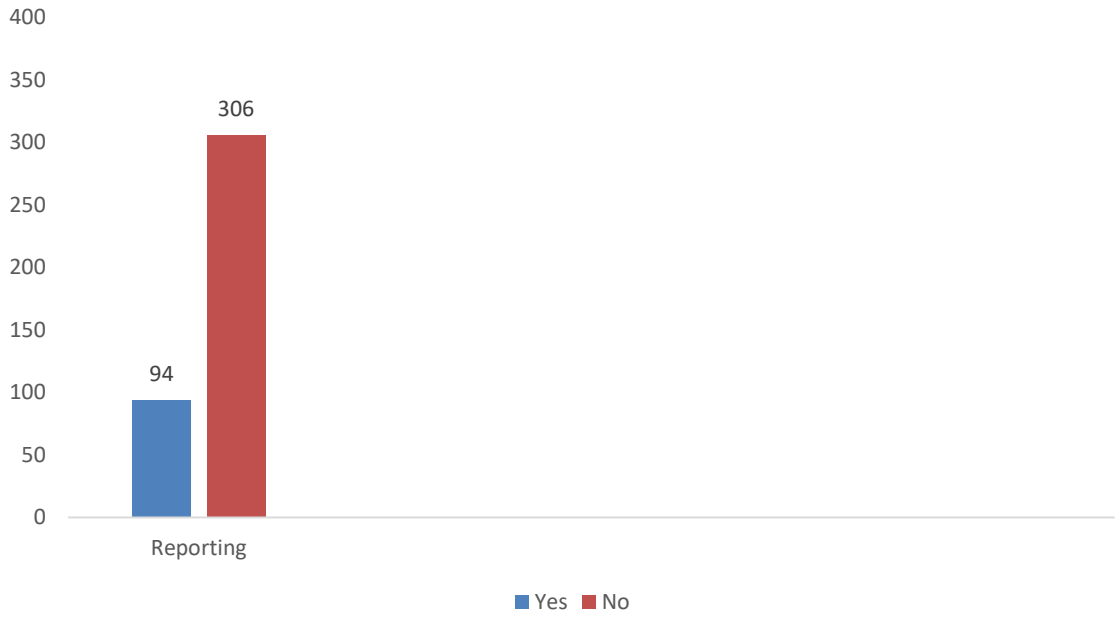
Figure 4.7 represents that 55 out of 400 respondents (13.75%) reside on campus and reported that they have been victimized or have fear of being cybercrime victimization but 89 out of 400 respondents (22.25%) being on campus negate this fact. In case of off campus residence but located in city 66 out of 400 respondents (16.5%) said that they have been victimized of cybercrime over the last six months, but 101 out of 400 respondents (25.25%) said they have not victimized of cybercrime being off campus reside in city. And finally in case of off campus in rural areas reside 23 out of 400 respondents (5.75%) reported that they have been victimized of cybercrime in last six months but 65 out of 400 (16.25%) respondents said that they are not victimized at all being reside off campus in rural areas. The ratios of not being victimized is quite

higher than the ratios of being victimized in all three above presented cases, thus the negative correlation of the residence in effect with cybercrime victimization has been evaluated.

4.2.2.7. Reporting to Law Enforcement Agencies

The cybercrime issue demands on time reporting to the law enforcement agencies in order to prevent this adverse problem from society. But contextual studies reveal that the people hesitate in reporting their issue. To evaluate the situation in Pakistan this study have tested the responses of victimized people either they reported to law enforcement agencies or not. The results have been show in figure 4.8.

Figure 4.8: Reporting to Law Enforcement Agencies if Victimized



According to the results (figure 4.8) 306 out of 400 respondents i.e. almost 77% told that they never reported to any law enforcement agency about their complaint of cybercrime. While rest

23% have try to complaint to agencies but they were not satisfied with the efficiency of these agencies.

4.2.2.8. Usage of Security software

To evaluate the results on either people use some security software to prevent the cybercrime issues or not 400 responses have been collected.

Figure 4.9: Usage of Security Software in Preventing Cybercrime Victimization

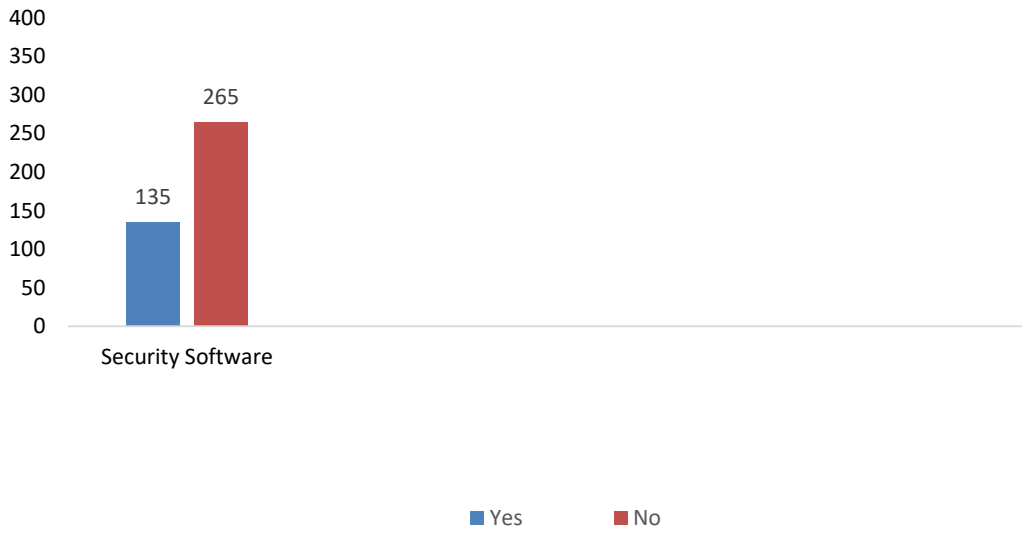


Figure 4.9 show that almost 66% of total respondents do not uses any type of security software. The remaining 33% used some kind of software including anti viruses.

4.3. Types of Cybercrimes Faced by Respondents

To evaluate the most dangerous type of cybercrime within which the respondents reported to be more victimized different types of cybercrimes have been listed and investigated from the targeted respondents. The frequencies and percentages of each of type of cybercrime have been presented in table 4.1.

Table 4.1: Types of Cybercrimes Faced by Respondents

Types	Frequency	Percentage
Phishing emails	7	3.52
Hacking of accounts	12	7.34
Threatening calls for photos uploading	43	22.01
Credit card based frauds	12	6.92
Stalking	21	15.71
Online harassment	35	18.01
Spam emails	26	14.01
Anonymous calls and SMS	53	26.34
Fake profile creation	59	28.72
Photo Circulation	33	16.09
Threatening about the Photo circulation	67	32.01

The Table 4.1 shows that the overall cybercrimes that victims are facing can be categorized as; Phishing emails, Hacking of accounts, Threatening calls for photos uploading, Credit card based frauds, Stalking, Online harassment, Spam emails, Anonymous calls and SMS, Fake profile creation, Photo Circulation and Threatening about the Photo circulation. Although, the women have been responded higher in this concern and out of all these crime two have been reveal to have comparatively higher frequency percentages. One is based on the online harassment for the reason of self-revenge or defamation and other is based on the cheating and frauds that are committed against women. The highest percentage of victims almost 32% are facing threats about their photo circulation on social media. 3% of the respondents receives the phishing emails on daily basis. Almost 7% of the respondents face the hacking of accounts and their accounts are used by criminals for different criminal activities. 22% of the respondents receive the threats of about their photos, these threats are either from the X husbands or relatives who want to take revenge from the respondent. Normally this kind of cybercrime activity is committed against women. Almost 26% of the respondents are receiving anonymous phone calls and SMS. 59% of the respondents face the issue of fake profile and misuse of their profiles.

Table 1.2: Respondents Frequency of Cybercrime

Types	**Frequency Percentage (Once)-Lowest**	**Frequency Percentage (Twice)-Moderate**	**Frequency Percentage (Thrice)=Highest**
Phishing emails	7 (3.80)	1 (0.39)	3 (1.05)
Hacking of accounts	28 (13.13)	1 (0.39)	2 (0.88)

Threatening calls for photos uploading	9 (4.12)	2 (0.88)	11 (4.24)
Credit card based frauds	6 (2.31)	-	2 (0.88)
Stalking	2 (0.88)	-	4 (2.32)
Online harassment	6 (3.31)	-	9 (4.12)
Spam emails	28 (13.20)	-	7(2.83)
Anonymous calls and SMS	21 (9.63)	7 (2.94)	26 (13.10)
Fake profile creation	26 (13.10)	1 (0.39)	4 (2.32)
Photo Circulation	34 (21.28)	4 (2.32)	9 (4.12)
Threatening about the Photo circulation	2 (0.88)	4 (2.32)	3 (1.46)

Considering the frequency of victimization (Table 4.2) cumulative score for all respondents is calculated. Based on the calculated score the lowest frequency (23.88%), moderate (31.23%) and highest (47.34%) is calculated.

4.4. Statistical Descriptions Using Statistical Calculations:

This section represents results and statistical analysis of all under consideration variables. All the calculations are performed via using statistical package of social sciences software.

4.4.1. Frequency Distribution:

Frequency distribution is used to organize the raw collected data in form of table or classes in order to present the results from that collected data (Manikandan, S. 2011). Here for this study frequency distribution has been presented for knowledge about cybercrime to the respondents,

activities respondents performed via different mediums, reason of the internet usage and the use of social networking sites by respondents. The details have been presented in following sections.

4.4.1.1. Knowledge about Cybercrime

Knowledge about cybercrime has been investigated in domains of two categories; cyber dependent crimes and cyber enabled crime in order to evaluate that either the respondents are aware of these terminologies or not.

Table 4.3: Knowledge about Cybercrime

Knowledge about Cybercrime	Frequency
Cyber dependent Crimes	39
Cyber enabled Crimes	24
Both	321
N=384	

400 respondents were targeted to get response on their 'know how' about their knowledge concerning cybercrime. Table 4.3 show that 384 active responses have been collected, out of them 39 respondents said that they are aware of cyber dependent crimes, 24 respondents said that they are aware of cyber enabled crime and 321 said that they know about both kinds of the crime.

4.4.2. Activities perform by respondents using Different Mediums

The data in concern of the activities performed on internet by the respondents via using different mediums has been collected in order to know the habit of the respondents to use the internet and

the results have been presented in table 4.4 regarding phone, tablet, laptop and desktop for the activities such as; social networking, shopping, sharing files, game playing, online banking, music downloading, chatting and emailing.

Table 4.4: Activities perform by respondents using different medium

	Phone %	**Tablet %**	**Laptop %**	**Desktop%**
Social networking sites	87.01	34.2	23.21	18.09
Shopping	3.01	11.90	10.98	4.89
Sharing files	2.09	45.09	64.09	63.12
Game Playing	78.01	67.09	53.23	43.01
Online Banking	46.01	32.01	67.19	64.22
Music Downloads	45.45	57.98	78.91	76.09
Chatting	76.98	45.90	43.01	34.01
Emailing	3.09	34.94	65.90	14.90

Statistics presented in Table 4.4 show that, almost 87% of the respondents prefer to use their phones to access the social networking sites while 34% uses tablet, 23% used laptop and 18% uses desktops. 3% respondents use phone for shopping, 11% of the respondents use tablets for performing shopping activities online, 10.98% people uses laptop and 4.89% uses desktop. 2.09% of the respondents use phone for sharing files, 45.09% use tablet, 64.09% use laptop and 63.12% use desktop for sharing files. For concern of game playing 78.01% respondents use phone, 67.09% use tablet, 53.23% use laptop and 43.01% use desktop. For online banking

46.01% respondents use phone, 32.01% use tablet, 67.19% use laptop and 64.22% use desktop. For music download 45.45% respondents use phone, 57.98% use tablet, 78.91% use laptop and 76.09% use desktop. For sake of chatting 76.98% respondents use phone, 45.90% use tablet, 43.01% use laptop and 34.01% use desktop. But for emailing 3.09% of the respondents use phone, 34.94% use tablet, 65.90% use laptop and 14.90% use desktop.

4.4.3. Reason of Internet Usage By respondents

The data has been collected for determining the reason of the using internet by the respondent in order to evaluate their causes and pattern of using internet to get knowledge about being victimized. The results have been presented in table 4.5.

Table 4.5: Reason of Internet Usage By respondents

Reasons	Frequency	Percentage
Social networking	65	24.63
Study	18	10.87
Online Billings	10	3.23
Official work	140	35.2
Staying in touch with family and friends	139	79.8

The statistics presented in table 4.2 show the reason of using internet by respondents. According to the calculations, 24.63% respondents use internet for social networking, 10.87% use for study, 3.23% use for online banking, 35.2 % use for official work and highest ratio 79.8% respondents use the internet for staying in touch with family and friends and according to the facts it is the zone from which most of the cyber victimized cases arouse.

4.4.4. Use of Social networking sites by respondents

For sake of results evaluation the data has been collected in concern of pattern of use of social sites by the respondents and the results have been presented in table 4.6.

Table 4.6: Use of Social networking sites by respondents

Social Network Sites (SNS)	Number	Frequency	Percentage
Number of accounts	One	101	70.92
	Two	29	22.01
	Three	9	3.09
Number of Years	Below 5	91	89.1
	5-10	12	6.20
	Above 10	4	1.3
Online Friends	Below 100	43	45
	100-200	9	5
	Above 200	2	0.91

The statistical value in Table 4.6 shows that 70% of the respondents have one account, 22% of them have two accounts and only 3% of the respondents have three accounts. 89% of the respondents are using SNS from less than 5 years, while 6% of the respondents are using these websites from less than 10 years and only 1.3% of the respondents have accounts that are older than 10 years. 45% respondents have below 100 online friends, 5% have the online friends ranging from 100 to 200 and only 0.91% respondents have online friends above 200.

4.5. Hypothesis testing:

In this section the proposed hypothesis (section 3.8) for this study has been tested via statistical analysis and interpreted according on basis of the collected data. There are five main hypotheses based upon the analytical framework and objective of the study (as presented in section 3.8. Hypotheses) but have been sub categories in multiple hypotheses according to need of result determination and evaluation; two sub categories for first hypothesis and seven sub categories for fifth hypothesis.

Hypothesis 1: knowledge about specific terminologies about cybercrime is sub-divided into two hypotheses.

- **Hypothesis $_{1A:}$** Null Hypothesis: "The knowledge about specific terminology is important."
- **Hypothesis $_{1B:}$** Null Hypothesis: "Students who have no knowledge about the fact that how cybercrime can be carried out can save themselves to become a victim of cybercrime"

Hypothesis $_{1A:}$ "The knowledge about specific terminology is important"

Table 4.7: Hypothesis$_{1A}$

Knowledge About Cybercrime terminology	Mean (M)	Standard Deviation (S.D)	t-value	p-value
cyber enabled	14.12	4.043	17.88	0.072
cyber dependent	18.87	9.324		

crimes				
Both				

Thus the null hypothesis is not rejected according to value p=0.072. Thus this shows that it does not make any difference that whether the respondent has knowledge about specific terminologies.

Hypothesis $_{1B}$: "Students who have no knowledge about the fact that how cybercrime can be carried out can save themselves to become a victim of cybercrime."

Table 4.8: Hypothesis$_{1B}$

Knowledge About Cybercrime	**Mean (M)**	**Standard Deviation (S.D)**	**t-value**	**p-value**
Well Aware	2.34	2.765	17.88	0.001
Not Aware	6.65	7.83		

The Table 4.8 the p-value is less than 0.05 which clearly rejects our null hypothesis and showing that there is significant difference between the less knowledge and being a cybercrime victim. Therefore the mean value for the victims who has no awareness about the cybercrime is quite high (M=6.65, S.D=7.83). The result shows that the respondents who do not have any knowledge about the cybercrime have more chances to become a cybercrime victim.

Hypothesis 2:

H_2: "Ratio of women is equal as compare to men in case of cybercrime victimization"

Table 4.9: Hypothesis 2

Gender	Mean (M)	Standard Deviation (SD)	t-value	p-value
Male	33.14	17.29	13.989	0.000
Female	48.05	25.97		

Source: Author's own findings

According to Table 4.9 the resultant p-value is 0.000 which is less than 0.05 which clearly rejects our null hypothesis, showing that there is significant relationship between the gender types and being a cybercrime victim. Therefore the mean value for the female respondents is quite high (M=48.05, SD=25.97). The result shows that the female respondents have more ratio as compare to men while being a victim of cybercrime.

Hypothesis 3:

H_3: "Students who are spending more time on internet have less risk to become a victim"

Table 4.10: Hypothesis 3

No of Hours On internet	Mean (M)	Standard Deviation (SD)	t-value	p-value
2-4	17.21	8.29	21.0998	0.0034
5-8	22.09	11.97		
More than 8	53.01	31.90		

According to Table 4.10 the resultant p-value is 0.0034 which is less than 0.05 which clearly rejects our null hypothesis, showing that there is significant relationship between the time spent on internet and being a cybercrime victim. Therefore the mean value for the respondents who spent more than 8 hours online is quite high (M=53.01, SD=31.90). The result shows that the respondents who spent more time on internet have more chances to become a cybercrime victim.

Hypothesis 4:

H_4: "Chances of sexual harassment and cyber bullying is not increase by only using social media or online other online resources."

Table 4.11: Hypothesis 4

Chances of Sexual Harassment and Cyber bullying because of using social media and online resources	Mean (M)	Standard Deviation (SD)	t-value	p-value
High	61.65	29.09	42.0654	0.000
Low	29.01	8.05		

According to Table 4.11 the resultant p-value is 0.000 which is less than 0.05 which clearly rejects our null hypothesis, showing that there is significant relationship between the harassment and social networking sites. Therefore the mean value (M=61.65, SD=29.09). For the respondents who have more activity on social networking sites have high chances of becoming a

cybercrime victim. The result shows that the spending more time by using social networking sites increases the chances of being a cybercrime victim.

Hypothesis 5:

H_5 Null hypothesis: There is no significant relationship between socio-demographic features and cybercrime victimization. The demographic consider here are marital status, income level, study level and location of residence.

Thus, this hypothesis is sub divided into seven hypotheses to present the results for each of the socio demographic features separately. Hence the sub-divided null hypotheses are as follows:

- **H_{5A}: Null Hypothesis: "**There is no significant relationship between marital status and cybercrime victimization".
- **H_{5B}: Null Hypothesis: "**There is no significant relationship between income level and cybercrime victimization."
- **H_{5C}: Null Hypothesis: "**There is no significant relationship between study level and cybercrime victimization."
- **H_{5D}: Null Hypothesis: "**There is no significant relationship between employment status and cybercrime victimization."
- **H_{5E}: Null Hypothesis: "**There is no significant relationship between residence location and cybercrime victimization."
- **H_{5F}: Null Hypothesis: "**There is no significant relationship between Age and cybercrime victimization."
- **H_{5G}: Null Hypothesis: "**There is no significant relationship between Gender and cybercrime victimization."

H_{5A}: "There is no significant relationship between marital status and cybercrime victimization."

Table 4.12: Hypothesis $_{5A}$

Marital Status	Mean	SD	p-value
Single	56.07	21.39	0.061
Married	48.91	19.81	
N=400			

According to Table 4.12 the p-value is 0.061 which is greater than 0.05. Hence out null hypothesis is not rejected and shows that there is no significant relationship between the marital status and being a cybercrime victim. So it means that whether a person is married or single it does not make any difference. Both of these types are facing cybercrime.

H_{5B}: "There is no significant relationship between income level and cybercrime victimization."

Table 4.13: Hypothesis $_{5B}$: Income level

Income Level	Mean	SD	p-value
Government Job	67.89	11.32	0.0721
Business	54.29	9.09	
N=400			

According to Table 4.13 the p-value is 0.0721 which is greater than 0.05. Hence out null hypothesis is not rejected and shows that there is no significant relationship between the income level and cybercrime victimization. People from any job type and income level are facing cybercrime. So this variable can be ignored.

H_{5C}: "There is no significant relationship between study level and cybercrime victimization."

Table 4.14: Hypothesis $_{5C}$ Study Level

Study Level	Mean	SD	p-value
Full Time	12.001	3.10	0.0508
Part Time	19.09	6.002	
N=400			

According to Table 4.14 the p-value is 0.0508 which is greater than 0.05. Hence out null hypothesis is not rejected and shows that there is no significant relationship between the study levels. Students belonging to full time or part time or both are facing cybercrime victimization. So this variable can be ignored.

H_{5D}: "There is no significant relationship between employment status and cybercrime victimization"

Table 4.15: Hypothesis $_{5D}$ Employment Status

Employment Status	Mean	SD	p-value

Not working	4.19	3.10	0.0009
Working Full time	21.09	11.002	
Working part time	16.003	7.92	

According to Table 4.15 the p-value is 0.0009 which is less than 0.05. Hence our null hypothesis is rejected and shows that there is significant relationship between the employment status and becoming a cybercrime victim. Results in table shows that the students who are working full time feel that they have been victimized more in terms of cybercrime activities.

H_{5E}: "There is no significant relationship between residence location and cybercrime victimization."

Table 4.16: Hypothesis $_{5E}$ Residence Location

Residence Location	Mean	SD	p-value
On campus	6.99	3.10	0.0621
Off campus city	11.34	6.002	
Off campus rural areas	14.09	6.98	
N=400			

According to Table 4.16 the p-value is 0.0621 which is greater than 0.05. Hence out null hypothesis is not rejected and shows that there is no significant relationship between the study location of residence and cybercrime victimization. So this variable can be ignored.

H_{5F}: "There is no significant relationship between Age and cybercrime victimization."

Table 4.17: Hypothesis $_{5F}$ Age

Age	Mean	SD	p-value
Under 20 years	7.087	3.10	0.00012
20-30	23.091	11.002	
31-40	14.981	5.98	
Above 40			
N=400			

According to Table 4.17 the p-value is 0.00012 which is less than 0.05.Hence our null hypothesis is rejected and shows that there is significant relationship between the age and becoming a cybercrime victim. Results in table shows that the students who have ages between 20 and 30 are facing more cybercrimes in daily life.

H_{5G}: "There is no significant relationship between Gender and cybercrime victimization"

Table 4.18: Hypothesis $_{5G}$: Gender

Gender	Mean	SD	p-value
Male	9.233	5.012	0.0007
Female	32.09	17.90	
N=400			

According to Table 4.18 the p-value is 0.0007 which is less than 0.05. Hence our null hypothesis is rejected and shows that there is significant relationship between the gender and becoming a

cybercrime victim. Results in table shows that the students who are females have becoming more cybercrime victims as compare to men.

4.5.1. Summary of the Hypotheses:

This section presents the summary of hypotheses with label of accepted or rejected. For this concern the accepted hypotheses symbolized with "✓"and rejected hypothesis symbolized with "x". There are five main hypotheses based upon the analytical framework and objective of the study (as presented in section 3.8. Hypotheses) but have been sub categories in multiple hypotheses according to need of result determination and evaluation; two sub categories for first hypothesis and seven sub categories for fifth hypothesis.

Table 4.19: Acceptance or Rejection of Hypotheses based on findings

	Research Hypotheses	Accepted/ Rejected
1	**"H_{1A}:** The knowledge about specific terminology of Cyber-Crime is not important.	x
2	**H_o:** The knowledge about specific terminology is important.	✓
3	**H_{1B}:** Students who have no knowledge about the fact that how cybercrime can be carried out cannot save themselves to become a victim of cybercrime	✓
4	**H_o:** Students who have no knowledge about the fact that how cybercrime can be carried out can save themselves to become a victim of cybercrime	X
5	**H_2:** Ratio of women and men is different in case of cybercrime victimization.	✓
6	**H_o:** Ratio of women is equal as compare to men in case of cybercrime	X

	victimization.	
7	**H_3:** Students who are spending more time on internet have more risk to become a victim.	✓
8	**H_o:** Students who are spending more time on internet have less/no-more risk to become a victim.	X
9	**H_4:** Chances of sexual harassment and cyber bullying increased by only using social media or online other online resources.	✓
10	**H_o:** Chances of sexual harassment and cyber bullying is not increase by only using social media or online other online resources.	X
11	**H_{5A}:** There is a significant relationship between marital status and cybercrime victimization.	X
12	**H_o:** There is no significant relationship between marital status and cybercrime victimization.	✓
13	**H_{5B}:** There is a significant relationship between income level and cybercrime victimization.	X
14	**H_o:** There is no significant relationship between income level and cybercrime victimization.	✓
15	**H_{5C}:** There is a significant relationship between study level and cybercrime victimization.	X
16	**H_o:** There is no significant relationship between study level and cybercrime victimization.	✓
17	**H_{5D}:** There is a significant relationship between employment status and cybercrime victimization.	✓

18	**H_0:** There is no significant relationship between employment status and cybercrime victimization.	X
19	**H_{5E}:** There is a significant relationship between residence location and cybercrime victimization.	x
20	**H_0:** There is no significant relationship between residence location and cybercrime victimization.	✓
21	**H_{5F}:** There is a significant relationship between Age and cybercrime victimization.	✓
22	**H_0:** There is no significant relationship between Age and cybercrime victimization.	X
23	**H_{5G}:** There is a significant relationship between Gender and cybercrime victimization.	✓
24	**H_0:** There is no significant relationship between Gender and cybercrime victimization."	X

Source: Author's own findings

Chapter 5

Conclusion and Recommendations

This chapter presents the key findings extracted from the results of this research study. These findings are generated by applying statistical testing to the respondent's data and findings presented in chapter 4 having the bar chart graphs, descriptive analysis and statistical description. This chapter presents the comprehensive discussion on results along with the findings, proposed policy based upon the findings and recommendations as well.

5.1. Knowledge/ Awareness and cybercrime victimization

Total 400 responses have been made out of them 4 respondents do not answer about awareness thus, 396 actual responses have been gathered. In concern of awareness about cyber enabled crime 95 out of 400 respondents' i.e. 23.75% said that they are just aware about cyber enabled crimes, 35 respondents out of 400 i.e. 8.75% reported that they are not aware of cyber enabled crimes. On the other hand in concern of cyber dependent crimes 127 respondents out of 400 i.e. 31.75% said that they are just aware about the cyber dependent crime and 81 respondents out of 400 i.e. 20.25% said that they are not aware about cyber dependent crime. And in terms of the awareness of the both kinds of the crimes 35 out of 400 respondents i.e. 8.75% said that they have awareness of both kinds of cyber-crimes but 23 out of 400 respondents' i.e. 5.75% reported that they are neither aware about cyber enabled crimes nor cyber dependent crimes (see Figure 4.1). The presented ratios depict that the awareness about the terminologies of the cybercrime among university students is quite low.

Also the hypothesis that is “the knowledge about specific terminology is important” is not rejected (Table 4.7, 4.8). Thus this shows that it does not make any difference that whether the respondent has knowledge about specific terminologies as well as the importance of being aware of the cybercrime terminologies is also presented to be important.

First hypothesis is based on the fact that respondents who have more knowledge can have less chances of being cybercrime victim (Van de Weijer and Leukdeldt 2017). According to the results the respondents who have less awareness about the types of cybercrimes and how these crimes are committed have more chances to become a cybercrime victim. The table shows the p-value is less than 0.05 which clearly rejects our null hypothesis and showing that there is significant difference between the less knowledge and being a cybercrime victim. The result shows that the respondents who do not have any knowledge about the cybercrime have more chances to become a cybercrime victim.

5.2. Gender type in Cybercrime victimization

Second hypothesis is designed to find out that which gender is more affected in case of cybercrime. The proposed hypothesis was based on the fact that “whether the ratio of women is equal to men in case of cybercrime victimization” (Donner, C. M., 2016). According to Table (4.9) the resultant p-value is 0.000 which is less than 0.05 which clearly rejects our null hypothesis, showing that there is significant relationship between the gender types and being a cybercrime victim. The result shows that the female respondents have more ratio as compare to men while being a victim of cybercrime. Moreover these results have become more accurate with the support of descriptive analysis i.e. according to the figure (4.2) among 400 respondents 88 male respondents i.e. 22% are those reported that they have been victimized of cybercrime

and 49 male respondents' i.e. 12.25% said that they have not been victimized of cybercrime. On the other hand in concern of the female respondents 157 female out of 400 respondents i.e. 39.25% said that they have been victimized of the cybercrime and 77 female respondents out of 400 i.e. 19.25% reported that they have not been victimized of cybercrimes. On collective basis, 61.25% respondents have been reported to be victimized by cybercrime with greater ratio of the female victims. Thus we can safely conclude that females are more victimized by cybercrime as compare to male.

5.3. Time and Cybercrime Victimization

Third hypothesis was based on "the relationship between the times spends online and chances of being a cybercrime victim".

The proposed null hypothesis was Students who are spending more time on internet have less risk to become a victim (Chao, C. M. and Yu, T. K. 2017). According to Table (4.10) the resultant p-value is 0.0034 which is less than 0.05 which clearly rejects our null hypothesis, showing that there is significant relationship between the time spent on internet and being a cybercrime victim. The result shows that the respondents who spent more time on internet have more chances to become a cybercrime victim.

Social networking sites increases the chances of cybercrime

The proposed null hypothesis is "Chances of sexual harassment and cyber bullying is not increase by only using social media or online other online resources".

According to Table (4.11) the resultant p-value is 0.000 which is less than 0.05 which clearly rejects our null hypothesis, showing that there is a significant relationship between the harassment and social networking sites. For the respondents who have more activity on social networking sites have high chances of becoming a cybercrime victim. The result shows that the spending more time by using social networking sites increases the chances of being a cybercrime victim.

5.4. Socio demographic features

This hypothesis is about "the relationship between Socio demographic features of respondents and cybercrime victimization". The proposed null hypothesis shows that there is no significant relationship between socio-demographic features and cybercrime victimization. The demographic consider here are marital status (Table 4.12), income level (Table 4.13), study level (Table 4.14), employment status (Table 4.15), location of residence (Table 4.16), age (Table 4.17) and Gender (Table 4.18). The results in this context shows that socio-demographic features including income level, residence location and study level does not have any direct relationship with the cybercrime victimization. On the other hand the marital status, employment status, age and gender have significant relationship with cybercrime victimization.

5.5. Types of Cybercrimes faced by respondents

The Table 4.1 shows that the overall cybercrimes that victims are facing can be categorized as; Phishing emails, Hacking of accounts, Threatening calls for photos uploading, Credit card based frauds, Stalking, Online harassment, Spam emails, Anonymous calls and SMS, Fake profile creation, Photo Circulation and Threatening about the Photo circulation. Although, the women

have been responded higher in this concern and out of all these crime two have been reveal to have comparatively higher frequency percentages. One is based on the online harassment for the reason of self-revenge or defamation and other is based on the cheating and frauds that are committed against women. The highest percentage of victims almost 32% are facing threats about their photo circulation on social media.3% of the respondents receives the phishing emails on daily basis. Almost 7% of the respondents face the hacking of accounts and their accounts are used by criminals for different criminal activities. 22% of the respondents receive the threats of about their photos, these threats are coming from the ex-husbands and relatives who want to take revenge from the respondent. Normally this kind of cybercrime activity is committed against women in 99% cases. Almost 26% of the respondents are receiving anonymous phone calls and SMS. 59% of the respondents face the issue of fake profile. With their names fake profiles are created and then misused.

According to table the frequency (4.2) of victimization cumulative score for all respondents is calculated. Based on the calculated score the lowest frequency (23.88%), moderate (31.23%) and highest (47.34%) is calculated.

5.6. Reporting Cybercrime to Law Enforcement Agencies

According to the results (figure 4.7) 306 out of 400 respondents i.e. almost 77% told that they never reported to any law enforcement agency about their complaint of cybercrime. While rest 23% have try to complaint to agencies but they were not satisfied with the efficiency of these agencies. Although, the cybercrime issue demands on time reporting to the law enforcement agencies in order to prevent this adverse problem from society. This non-reporting by the victims

is the major factor of increase of the cybercrimes and thus the frauds, hacking and harassment is increasing day by day. (Van de Weijer, S. G. et al., 2018)

5.7. Usage of Security Software

Figure 4.8 show that almost 66% of total respondents do not uses any type of security software. The remaining 33% used some kind of software including anti viruses. Although, they should use the security software as precautionary measure of being hacked and frauds but many of the respondents claim that the free available software are of no value to protect them and the paid software are international based and not easily accessed as well as not affordable by many of the web users.

5.8. Findings

We have the following key findings in the context of our proposed research.

- Most of the cybercrime victims are female between the ages of 20 and 30.
- Most of the offenders are relatives or the people who already knows the victims. Like in case of divorced women offenders are their ex-husbands.
- Divorced women have faced more cybercrimes in terms of sexual harassment
- The major reason for being cybercrime victim is less knowledge about the internet and less usage of security measures like firewall and strong passwords.
- There are many other reasons for cybercrime victimization which includes no defined laws and rules against the criminals. So women in Pakistan do not have any confidence about the fact that, how they can report against the offenders.
- Less security measures are applied by female users when they are using Facebook and twitters accounts .Most of them do not know about the security settings available.

- Spending more time on social networking sites increases the chance of being a victim of cybercrime like cyber bullying and online harassment.
- Students are not using any updated anti viruses and security software because they do not know the importance of this software.
- Most of the women who are victim of cybercrime does not report it to the concerning agencies because they feel ashamed. And also they do not have any confidence about the efficiency and procedures of these agencies.
- Women present in cyberspace are confronting the different types of cybercrime exploitation, for example, photograph circulation, mysterious calls of profane nature, web based hacking and abuse, counterfeit profile, maligning, undermining calls, pantomime by hacking, provocation, transforming, phishing emails, stalking, online harassments and so on.
- As compare to married women, single women spent more time on internet and more friends on social media websites that's why they become more victims of cybercrime.
- Therefore whatever the study level is all people are using spending same amount of time on internet.
- Most of the time internet is used by phones which are not safe way to access the private information and there are more chances that information can be hacked easily.

5.9. Proposed Policy:

It is exposed from the contextual studies and evidences that the current cybercrime prevention measure being practicing in Pakistan is the "Prevention of Electronic crime Act 2016". Although the act was quite comprehensive in papers and covers all domains of cyber-crimes. But this law has been called out controversial and ambiguous from many of blogs and research articles (Khan, E. A., 2019; Farieha Aziz, 2018; Mehreen Zehra Malik, 2016; Raza Khan, 2016;

Shamama Tul Amber 2016), the reason fall in the non-confidentiality reporting by the women victimization and of course the impracticality of the law based upon the penalties presented in it. Thus after doing a detailed research on this serious issue it is revealed that there is a need of devising a certain policy which is easy to implement and near to provide justice with all confidentialities. For sake of devising any of the public policy it needs the support of public policy theory.

5.9.1. Public Policy Theory:

The policy making needs the support of public policy theory, as policy making could never be happened in vacuum it needs the support of the public policy theory (Kitchelt, H., 1986). The public policy is concerned with the government anticipation in achieving a certain goal for benefit of the common people and the state (Anyebe, A.A., 2018). According to Anyebe, (2018), public policy making involves certain theories depends upon the reason of the policy making; elite theory, group theory, system theory, institutional theory, incremental theory, and rational choice theory. As per the concern of this study, the under discussion study have its roots in system theory because, the system theory includes the legal compliances, rules and regulations, judicial decisions and the law making etc. System theory helps in policy making process by receiving input from the environment and then converting the demands of the environment into the output by presenting some outcomes by making sure that those outcomes reflect the determination of the social morals and values, these outcomes specifically stated as the policy outcomes. In more specific persona the system theory consider the public policy as the reaction to the political system demanding something from environment having authoritative allocations with ultimate goal of the societal improvements (Anyebe, 2018). This study follows the same rule as the issue of cybercrime victimization is causing a societal problem and affecting the

society in a negative way. Although the existing measures to prevent the cybercrime do not working adequately, by having inputs from the environment concerning the issue of the cybercrime this study have presented the clear results and is about to present a policy as an outcome of the results to bring improvement in domains of cybercrime by minimizing them eventually. From this spectrum by having the results of the study, their interpretation and discussion it is suggested that there should be a cyber-crime unit in each of the police station for getting grievances of cybercrimes and examination of cybercrimes on time as well as on doorstep. Because, most of the women victimized has been revealed from the study thus more female officers should be part of cybercrime units as the presence of more female officers in cybercrime units may urge more female casualties to come forward and hold up their grievances with no fear of optional exploitation. FIA and police cyber units must be collaborated with each other in order to make the police cyber units more educated in this domain. And extreme to all these, the confidentiality of the victim must be passed out on highest interest to protect their esteem. The penalties of the harassers and cyber terrorists must have practicality and the prison punishment must be ensured without any bail.

5.10. Recommendations

The recommendations of this study have hands in hand with the proposed policy and key findings presented before.

- In the curriculum of schools and colleges, the information about the cybercrimes should be elaborated.
- Different free training sessions should be conducted in order to create awareness about the prevention of these crimes and also how one can save from being a victim of cybercrime.

- There should be a mandatory cybercrime unit in each police station for getting grievances of cybercrimes and examination of cybercrimes.
- The presence of more female officers in cybercrime units may urge more female casualties to come forward and hold up their grievances with no fear of optional exploitation.
- The cybercrime casualties ought to be educated about their rights and cybercrime laws. It is the obligation of the cybercrime cell to give confidence to the people so that they can come forward with their issues.
- The law enforcement agencies should empower that all police officers ought to be given an essential education on web and media transmission administrations, with the goal that they can have the essential comprehension of cybercrimes. Those officers who are managing cybercrimes ought to be given periodical inside and out preparing projects to keep them refreshed and in fact skillful to research the rising types of cybercrimes.

REFERENCES:

A.N. Gulam Muhammad Kundi, Nawaz, A., Akhtar, R., & MPhil Student, I. E. R. (2014). "Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries." *Journal of Information Engineering and Applications*, *4*(4), 61-71.

Abrams, L. S. (2010). "Sampling 'hard to reach'populations in qualitative research: The case of incarcerated youth." *Qualitative Social Work*, *9*(4), 536-550.

Agency, N. C. (2018). "Crime report". Retrieved from http://www.nationalcrimeagency.gov.uk/.

Alvi, M. H. (2016). "A manual for selecting sampling techniques in research."

Andrews, D., Nonnecke, B., & Preece, J. (2007). "Conducting research on the internet:: Online survey design, development and implementation guidelines."

Anyebe, A. A. (2018). "An Overview of Approaches to The Study of Public Policy." *e-Bangi*, *15*(1).

Arfi, N., & Agarwal, S. (2014). "Knowledge of cyber crime among elderly across gender." *International Journal for Advance Research in Engineering and Technology*, *2*(2), 7-9.

Baker. (2011). "The Economic Impact of Cybercrime and Cyber Espionage". Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage.

Bhattacharyya, O., Reeves, S., & Zwarenstein, M. (2009). "What is implementation research? Rationale, concepts, and practices". *Research on Social Work Practice, 19*(5), 491-502.

Blogs, M. C. (2014). "*Microsoft takes on global cybercrime epidemic in tenth malware disruption*." Retrieved from https://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption/.

Blumberg, B., Cooper, D. R., & Schindler, P. S. (2008). "*Business research methods"* (Vol. 2). London: McGraw-Hill Higher Education.

Blumberg, B., Cooper, D.R., Schindler, P.S., (2014). "Business Research Methods" , 4th Revised edition edition. ed. McGraw Hill Higher Education, London.

brief., K. T. H. t. c. (2005). „High tech crime brief."

Bryan-Low, C. (2012). "Hackers-for-hire are easy to find". *Wall Street J.*

Button, M., Tapley, J., & Lewis, C. (2013). The "Fraud Justice Network and the infra-structure of support for individual fraud victims in England and Wales". *Criminology and Criminal Justice, 13,* 37–61.

Carson, M. C. S. (2001). "*Toward a framework for assessing data quality"* (No. 1-25). International Monetary Fund.

Chao, C. M., & Yu, T. K. (2017). "Associations among different internet access time, gender and cyberbullying behaviors in Taiwan's adolescents". *Frontiers in psychology, 8,* 1104.

Chen, Q., & Bridges, R. A. (2017, December). "Automated behavioral analysis of malware: A case study of wannacry ransomware". In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 454-460). IEEE.

Chilisa, B., & Kawulich, B. B. (2012). "Selecting a research approach: paradigm, methodology and methods." *Doing Social Research, A Global Context. London: McGraw Hill*.

Churchill, G. A., Brown, T. J., & Suter, T. A. (1996). "Basic marketing research."

Clemmitt, M. (2006, July 28). "Cyber Socializing: Are Internet Sites like MySpace potentially dangerous?" CQ Researcher, 16(27), 625-648.

Cohen, L. E., & Felson, M. (1979). "Social change and crime rate trends: A routine activity approach." *American sociological review*, 588-608.

Collis, J., & Hussey, R. (2009). "A Practical Guide for Undergraduate and Postgraduate Students."

Commission, E. (2018). "*Seurity Union: Commission steps up efforts to tackle illegal content online*. European Commission."

Corporation, S. (2013). "*Internet Security Threat Report".* Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf.

Costigan, C. L., & Cox, M. J. (2001). "Fathers' participation in family research: Is there a self-selection bias?". *Journal of family psychology*, *15*(4), 706.

Creswell, J. (1994). “Research design: Qualitative & quantitative approaches.” Thousand Oaks, CA: Sage

Creswell, J. W. (2017). “*Qualitative inquiry and research design: Choosing among five approaches*.” Sage publications.

Crowther, A. (2017). “National Defense and the Cyber Domain.” *Retrieved from The*. https://www.heritage.org/sites/default/files/201709/2018_IndexOfUSMilitaryStrength_CROWTHER.pdf

Daily, C. (2013). “Two stand trial for major phone scam in Shanghai.” Retrieved from usa.chinadaily.com.cn/epaper/2013-09/11/content_16961084.html.

Dijk, J. V., Kesteren, J. V., & Smit, P. (2007). “*Criminal victimisation in international perspective*.” Boom Juridische Uitgevers.

Donner, C. M. (2016). “The gender gap and cybercrime: An examination of college students’ online offending.” *Victims & Offenders*, *11*(4), 556-577.

Duggan, M. (2014). “*Online harassment*.” Pew Research Center.

Evans, M. (2016). “Cyber crime: One in 10 people now victim of fraud or online offences, figures show.” Crime correspondent 21 JULY 2016.

Farieha Aziz. (2018). “Paksitan’s Cybercrime Law: Boon or Bane?”. 14 Feb, 2018. Retrived from: https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

Foundation, D. R. (2016). “Online Harrasment Report.” https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf

Furnell, S., & Emm, D. (2017). “The ABC of ransomware protection.” *Computer Fraud & Security, 2017*(10), 5-11.

Ghauri, I. (2014). “Electronic Crimes Act: Cybercrime to be made non-cognisable offence,.” Retrieved from http://tribune.com.pk/story/672721/electronic-crimes-act-cybercrimeto-be-made-non-cognisable-offence/

Giddings, L. S. (2006). “Mixed-methods research: Positivism dressed in drag?”. *Journal of research in nursing, 11*(3), 195-203.

Goodman, M. (2010). “*Cyber Security, Transhumanism, & Future Crimes”.* Retrieved from https://blog.bulletproof.com/marc-goodman-cyber-security-transhumanism-future-crimes-203/.

Gordon S., F., R. (2004). “Cyberterrorism? In: Cybterterrorism.”

Goucher, W. (2010). “Being a cybercrime victim. *Computer Fraud & Security*”. *2010*(10), 16-18.

Greene, J. A., & Azevedo, R. (2007). “A theoretical review of Winne and Hadwin’s model of self-regulated learning: New perspectives and directions.” *Review of educational research, 77*(3), 334-372.

Griffen, R. (2008). “Is the Internet Safe Anymore?”. Retrieved from http://www.suzylamplugh.org/2014/09/Internet-safe-women-anymore

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). “Multivariate data analysis: A global perspective”. (Vol. 7).

Halder, D. (2014). “Information technology act and cyber terrorism: A critical review.” http://www.academia.edu/945156/Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review

Haque , P. (2013). “Pakistan Internet Use Survey 2013.” Retrieved from https://tribune.com.pk/story/591004/pakistan-internet-use-survey-2013/

Hassan, Z. A., Schattner, P., & Mazza, D. (2006). “Doing a pilot study: why is it essential?.” *Malaysian family physician: the official journal of the Academy of Family Physicians of Malaysia*, *1*(2-3), 70.

Helweg-Larsen, K., Schütt, N., & Larsen, H. B. (2012). “Predictors and protective factors for adolescent Internet victimization: Results from a 2008 nationwide Danish youth survey”. *Acta Paediatrica*, *101*(5), 533-539.

Holt, T. J., & Kilger, M. (2012). “Examining willingness to attack critical infrastructure online and offline”. *Crime & Delinquency*, *58*(5), 798-822.

Huff, R., Desilets, C., & Kane, J. (2010). “National public survey on white-collar crime.” *Retrieved October*, *28*, 2012.

Hunt, E. (2016). “Online harassment of women at risk of becoming'established norm', study finds.” *The Guardian*, *7*.

investigation, F. b. o. (2015). *"Internet crime report*." Retrieved from https://pdf.ic3.gov/2015_ic3report.pdf.

J. Toby Mordkoff. (2016). "Descriptive Statistics." *Copyright©2000.*

Jahankhani, H. (2013). "Developing a model to reduce and/or prevent cybercrime victimization among the user individuals." In *Strategic Intelligence Management* (pp. 258-268). Butterworth-Heinemann.

Jamil.Z. (2006). "*Cyber Law*. Pakistan: 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference". Retrieved from http://jamilandjamil.com/wp content/uploads/2010/11/article_for_scp_50_anniv_v5.0.pdf.

Jaquire, V., & von Solms, B. (2015). "A Strategic Framework for a Secure Cyberspace in Developing Countries with Special Emphasis on the Risk of Cyber Warfare." *International Journal of Cyber Warfare and Terrorism (IJCWT), 5*(1), 1-18.

Jfermiller. (2010). "jlmillersnotes.wordpress.com."

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2013). "Online harassment in context: Trends from three youth internet safety surveys (2000, 2005, 2010)". *Psychology of violence, 3*(1), 53. Journal of Computer Science, Volume V, 435-439.doi://10.26562/IRJCS.2018.AUCS10080

K, C. (2009). *"Cyber civil rights*." (89).

Kemp, S. (2018). "Digital in 2018: World's Internet Users Pass the 4 Billion Mark." Jan, 30th 2018. https://wearesocial.com/blog/2018/01/global-digital-report-2018

Khan, E. A. (2019). “The Prevention of Electronic Crimes Act 2016: An Analysis.” LUMS Law Journal.

Kimberly J. Mitchell ∗, J. W., David Finkelhor. (2008). “Are blogs putting youth at risk for online sexual solicitation or harassment?” *Child Abuse & Neglect*(32), 277–294.

Kitschelt, H. (1986). “Four theories of public policy making and fast breeder reactor development.” *International Organization, 40*(1), 65-104.

Krejcie, R. V., & Morgan, D. W. (1970). “Determining sample size for research activities.” *Educational and psychological measurement, 30*(3), 607-610.

Kshetri, N. (2006). “The simple economics of cybercrimes”. *IEEE Security & Privacy, 4*(1), 33-39.

Kundi, G. (2010). “E-Business in Pakistan: Opportunities and Threats.” from Lap-Lambert Academic Publishing

Leedy, P. (1997). “Practical research: Planning and design” (6th ed.). Columbus, OH: Prentice Hall.

Leedy, P. D., & Ormrod, J. E. (2005). “*Practical research”*. Pearson Custom.

Madhava S.S.P., U., S. (2011). “Information Technology Act and cyber terrorism: A critical review.” Cyber Crime and Digital Disorder,. In: Publications Division, Manonmaniam Sundaranar University.

Maimon, D. D. (2018). “Researchers Exposing the Human Side of Cybercrime.” Retrieved from https://bsos.umd.edu/feature/researchers-exposing-human

Manikandan, S. (2011). "Frequency distribution." *Journal of pharmacology & pharmacotherapeutics*, *2*(1), 54.

Manjikian, M. M. (2010). "From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik." *International Studies Quarterly*, *54*(2), 381-401.

Markoff, J. (2010). "Economic Impact of Cybercrime—No Slowing Down." Retrieved from https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Masud Ahmed Malik. (2018). "*Preventing Cybercrime: A Criminological Perspective*."

Mattoo, H. a. (2013). "The Internet, Cross-Border Data Flows and International Trade." *Issues in Technology Innovations*.

McAfee. (2018). "There's Nowhere to Hide from the Economics of Cybercrime." Retrieved from https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

McGuire, M., & Dowling, S. (2013). "Cyber crime: A review of the evidence. *Summary of key findings and implications." Home Office Research report*, *75*.

McGuire, M., & Dowling, S. (2013). "Cybercrime a review of the evidence (Research Report 75)." Chapter 4: Improving the cybercrime evidence base. Retrieved from www.gov.uk/government/ uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf

McKenna, K. Y. A., & Bargh, J. A. (2000). "Plan 9 from cyberspace: The implications for personality and social psychology." Personality and Social Psychology, 4(71).

Mehreen Zahra- Malik. (2016). “Pakistan Passes Controversial Cyber-crime law.” August 12th 2016. Retrieved from: https://www.reuters.com/article/us-pakistan-internet/pakistan-passes-controversial-cyber-crime-law-idUSKCN10N0ST

Memon, J. A. a. S. (2013). “Threats of Cyber Security and Challenges for Pakistan.” Paper presented at the 11th International Conference on Cyber Warfare and Security, USA. https://www.researchgate.net/publication/318850748_Threats_of_Cyber_Security_and_Challenges_for_Pakistan

Meško, G. (2018). “On Some Aspects of Cybercrime and Cybervictimization.” *European Journal of Crime, Criminal Law and Criminal Justice*, *26*(3), 189-199.

Mirza, J. (2013). “Pakistan takes steps to protect itself from NSA-style cyber attacks.” The News

Misra, A. P., Sherry M Jacob. (2010). “Women seen as soft targets for cyber crime.” Retrieved from http://economictimes.indiatimes.com/womenseen-as-soft-targets-for-cyber-crime/the-rate-of-cyber-crime-against-womenis-increasing-at-an-alarming-rate-in-india-/slideshow/5657973.cms

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2008). “Are blogs putting youth at risk for online sexual solicitation or harassment?”. *Child Abuse & Neglect*, *32*(2), 277-294.

Mohajan, H. K. (2017). “Two criteria for good measurements in research: Validity and reliability.” *Annals of Spiru Haret University. Economic Series*, *17*(4), 59-82.

Mohiuddin. (2015). “Cyber Laws in Pakistan.” http://supremecourt.gov.pk/ijc/articles/10/5.pdf (accessed on 5th March, 2015).

Najam, A., & Bari, F. (2017). “Pakistan National Human Development Report. Unleashing the Potential of a Young Pakistan”.

Nations, U. (1995). “The united Nations manual on the prevention and control of computer related crime”. International Review of Criminal Policy.

Navneet K,. (2018). “INTRODUCTION OF CYBER CRIME AND ITS TYPE”. IRJCS:: International Research

Neuman, W. L. (2013). “*Social research methods: Qualitative and quantitative approaches*.” Pearson education.

Nolan, S. (2012). “Huge spike in online dating after Christmas as holiday spirit encourages thousands to cure their loneliness.” Retrieved from www.dailymail.co.uk/news/article-2254968/Onlinedating-statistics-Huge-spike-Christmas-holiday-spirit-encourages-thousands-cure-loneliness. html#axzz2K7uODPC

Norton. (2012). “Norton cybercrime report”. Retrieved from http:\us.norton.com

Now, A. o. C. O. f. R. (2017). “Protecting Yourself in the Wake of the Equifax Data Breach.” Retrieved from https://www.acorn.org/article-list/protecting-yourself-in-the.html

Office, H. (2013b). “Commercial Victimisation Survey”. Retrieved from. https://www.gov.uk/government/publications/crime-against-businesses-detailed-findings-from-the-2012-commercial-victimisation-survey

Oksanen, A., & Keipi, T. (2013). “Young people as victims of crime on the internet: A population-based study in Finland.” *Vulnerable children and youth studies*, *8*(4), 298-309.

Pakistani, P. (2013). "Official Website of NADRA E-Sahulat Gets Hacked, User Data Compromised."

Paternoster, N. a. (2011). "Cybercrime Victimization: An examination of Individual and Situational level factors." International Journal of Cyber Criminology, 5(1).

Patton, M. Q. (2002). "Qualitative research and evaluation methods." Thousand Oaks. *Cal.: Sage Publications*.

Patton, M. Q., & Cochran, M. (2002). "A guide to using qualitative research methodology."

Piazza, P. (2006). "Technofile: Antisocial networking sites." *Security Management*, 1-5.

POULSE, K. P. (2018). "THE DECADE'S 10 MOST DASTARDLY CYBERCRIMES." Retrieved from https://www.wired.com/2009/12/ye-cybercrimes/ PWC. (2018). Staying vigilant – or turning a blind eye,fraud survey Retrieved from https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

Pring, R. (2000). "The 'false dualism'of educational research." *Journal of Philosophy of Education*, *34*(2), 247-260.

Qarar, S. (2018). "Cybercrime reports hit a record high in 2018: FIA." Dawn news report 23rd Oct, 2018. https://www.dawn.com/news/1440854

Raza Khan. (2016). "Controversial Cybercrime Bill Approved by NA." April 13th, 2016. Retrieved from: https://www.dawn.com/news/1251853

Remenyi, D., Williams, B., Money, A., & Swartz, E. (1998). "*Doing research in business and management: an introduction to process and method*." Sage.

Rubin, A., & Babbie, E. (2010). “Research methods for social work Belmont.” *CA: Thomson Brooks/Cole*.

Russell G. Smith, R. C.-C. C., Laurie Yiu-Chung Lau. (2015). “*Introduction: Cybercrime Risks and Responses — Eastern and Western Perspectives, Cyber crime risk and repsonses*: Palgrave Macmillan”.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). “Cyber-crimes and their impacts: A review.” *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Sarah Gordon • Richard Ford, J. C. V. (2006). “On the definition and classification of cybercrime.” springer, 13–20.

Saunders, J. (2017). “Tackling cybercrime–the UK response.” *Journal of Cyber Policy*, *2*(1), 4-15.

Saunders, M. N., & Lewis, P. (2012). “*Doing research in business & management: An essential guide to planning your project*.” Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2009). “*Research methods for business students*.” Pearson education.

Security, P. (2011). “A radical change in malware.” Retrieved from ps://www.pandasecurity.com/enterprise-cms3/security-info/cybercrime/.

Shamama Tul Amber. (2016). “Critics highlight the Issue in Cybercrimes Bill Passed by NA”. August 12, 2016. Retrieved from: https://dailytimes.com.pk/64033/critics-highlight-issues-in-cyber-crime-bill-passed-by-na/

Smith, R. G. I. Y. J., & M. Yar (Eds.),. (2010). “Identiy theft and fraud. Handbook of internet crime.” In (pp. 273-301). Cullompton, England: Wiley.

Staksrud, E., O ´lafsson, K., & Livingstone, S. (2013). “Does the use of social networking sites increase children’s risk of harm?” Computers in Human Behavior,, 29.

Statista. (2018). “Number of monthly active Facebook users worldwide as of 1st quarter 2018 (in millions).” Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Statistics, A. B. o. (2014). “Personal fraud costs Australians $1.4 billion.” Retrieved from www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument.

Statistics, I. W. (2016). “Internet user statistics.” Retrieved from https://www.internetworldstats.com/stats.html

Sultan Ullah, M. A., Mudasser Hamid Asmat, Kamran Habib. (2015). “Pakistan and Cyber Crimes: Problems and Preventions.” Paper presented at the First International Conference on Anti-Cybercrime.

Tashakkori, A., Teddlie, C., & Teddlie, C. B. (1998). “*Mixed methodology: Combining qualitative and quantitative approaches”.* (Vol. 46). Sage.

Telecommunication, W. (2017). “Measuring the Information Society Report”. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

Thompson, C. B. (2009). “Descriptive data analysis.” *Air medical journal*, *28*(2), 56-59.

Usman, M. (2016). “Cyber Crimes: A case study of legislation in Pakistan in the light of jurisdiction.” A dissertation to fulfill the corporate law degree.

van de Weijer, S. G., & Leukfeldt, E. R. (2017). “Big five personality traits of cybercrime victims.” *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412.

van de Weijer, S. G., Leukfeldt, R., & Bernasco, W. (2018). “Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking.” *European Journal of Criminology*, 1477370818773610.

Van der Meulen, N. (2010). “The Facilitation of Financial Identity Theft in the United States and the Netherlands.”

Viano, E. C. (2006). “Cybercrime, Organized Crime, and Societal Responses”. Springer.

Vosloo, J. J. (2014). “*A sport management programme for educator training in accordance with the diverse needs of South African schools”.* (Doctoral dissertation).

Wall, D. S. (2007). “Cybercrime.”

watch, C. (2011). “Cyber Crime Statistics.” Retrieved from http://www.cybercrimes watch.com/tag/cyber-crime-statistics/

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J. L. (2017). “Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap.” *Deviant Behavior*, 1-16.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006). “Online victimization of youth: Five years later.” later., & Bulletin., N. C. f. M. a. E. C. (2006). *Online victimization of youth: Five years later.*

Y. H. Mujahid. (2002). “Digital opportunity initiative for Pakistan.” The Electronic Journal of Information Systems in Developing Countries,, 8.

Yang. (2006). “A Review of Research Methodologies in International Business.” International Business Review.

Yazdanifard, R., Oyegoke, Tele, Seyedi, Arash Pour. (2011). “Cyber-crimes: Challenges of the Millennium Age.” Advances in Electrical Engineering and Electrical Machines. *springer,* 527-534.

Ybarra, M. L. (2004). “Linkages between depressive symptomatology and Internet harassment among young regular Internet users.” Cyberpsychology & Behavior, 7.

Zareen, M. S., Akhlaq, M., Tariq, M., & Khalid, U. (2013, December). “Cyber security challenges and wayforward for developing countries.” In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 7-14). IEEE.

Zeviar-Geese. (2005). “The state of the law on cyber jurisdiction and cybercrime on the internet.In: California Pacific School of Law.” Gonzaga Journal of International Law, 1, 1997-1998.

APPENDICES

Annex-1

Questionnaire

Cybercrime in Pakistan: Detection and Punishment Mechanism

I am Ubair Anjum, a research scholar from Pakistan Institute of Development Economics (PIDE), Islamabad, and currently working on my research dissertation. I am investigating on theme of "Cybercrime in Pakistan: Detection and Punishment Mechanism". I need a few minutes of your precious time, to help me complete this questionnaire. Your valuable input is of considerable and immense importance to me. I ensure you, that the data gathered and results generated shall only be use for research purposes. I assure you about high standards of research ethics and would respect your privacy.

Before completing the questionnaire, kindly read the scale provided. It shall serve as a guide to aid you in being better able to complete the form.

Name of Your Institute (Mandatory): _____

1. Gender

□ Male	□ Female

2. Please mention your age group

□ Under 20 Years	□ 20-30 Years	□ 31-40 years	□ Above 40

3. Please demonstrate your current marital status?

□ Single	□ Married	□ Divorced	□ Widow

4. What best depicts your present employment status?

□ Not Working	□ Working

5. What is the level of your study?

□ Full Time	□ Part Time

6. What constitutes cybercrime? Answers included "cybercrime executed by utilizing PC or its frameworks as the apparatus (cyber enabled)", "Violations conferred utilizing PC or its frameworks as the objective (cyber dependent)", or both.

7. How much time you spent on internet.

□ 2-4 Hours	□ 5-8 Hours	□ More than 8 Hours

8. Tick the cybercrime you face in last few years?

□ Phishing emails

□ Hacking of accounts

□ Threatening calls for photos uploading

□ Credit card based frauds

□ Stalking

□ Online harassment

□ Spam emails

□ Anonymous calls and SMS

□ Fake profile creation

□ Photo Circulation

□ Threatening about the Photo circulation

9. What is the most cybercrime activity you are facing on daily basis presenting in question 8? Pen down it.

10. Are you using any security software on your computer?

- Yes
- No

11. From which medium you perform most of your internet activity

Phone	Tablet	Desktop	Laptop

12. Do you think that Chances of Sexual Harassment and Cyber bullying increases because of using social media and online resources?
    - Yes
    - No

13. How many Facebook accounts you have?
    - One
    - Two
    - Three

14. How many Facebook friends you have?
    - Below 100
    - 100-200
    - Above 200

15. How long you have been using social networking sites?
    - Below 5 years
    - 5 to 10 years
    - Above 10 years

16. Do you know about the cyber laws in Pakistan?
    - Yes
    - No

17. Have you ever report to law enforcement agency?

- Yes
- No

18. Is it important to report the crime controlling agencies in case you are facing cybercrime in any form and if no then why not?
    - Yes
    - No

If no, state the reason here _____

19. During the past six months you face any cybercrime, if yes then what are the details about that?
    - Yes
    - No

If yes, state the detail here _____

20. Indicate the reason of using internet?

Social networking	Study	Online Billings	Official Work	Staying in touch with family and friends

21. Do you have any knowledge about the security setting of your online profiles?
    - Yes
    - No

22. Do you feel any need to install software like anti-virus, firewalls and spywares?
    - Yes
    - No

23. What do you feel that what is the reason behind the cyber victimization

□ Entertainment	□ Financial Gain	□ Hatred	□ Anger	□ Revenge

24. What are the different mediums offenders use to access you?

□ SMS	□ E-mail	□ Messengers	□ Social Networking Sites

25. Is there any relationship between the offender and you?

□ Yes

□ No

If yes, state the detail here _____

Annex-2

List of Targeted Universities

SR. Number	List of Top Ranked Universities
1	Quaid-i-Azam University
2	University of the Punjab
3	COMSATS Institute of Information Technology
4	University of Karachi
5	Pir Mehr Ali Shah Arid Agriculture University
6	Lahore University of Management Sciences
7	Government College University [Faisalabad
8	University of Peshawar
9	Bahauddin Zakariya University
10	Pakistan Institute of Development Economics
11	Islamia University
12	Riphah International University
13	International Islamic University
14	Government College University (Lahore)

15	University of Management and Technology
16	University of Faisalabad
17	Abdul Wali Khan University
18	University of Sargodha
19	University of Malakand
20	Forman Christian College
21	National University of Computer and Emerging Sciences
22	University of Azad Jammu and Kashmir
23	Bahria University
24	University of Gujrat
25	Kohat University of Science and Technology
26	National Defence University
27	Lahore College for Women University
28	Hazara University
29	University of Lahore
30	National University of Modern Languages