ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

# International Journal for Electronic Crime Investigation

# (IJECI)

VOL: 4
ISSUE: 4 Year 2020

Email ID: ijeci@lgu.edu.pk

Digital Forensics Rcscarch and Service Center
Lahore Garrison University, Lahore, Pakistan.

**LGU International Journal for Electronic Crime Investigation**
Volume 4(4) Year (2020)

## SCOPE OF THE JOURNAL

The IJECI is an innovative forum for researchers, scientists and engineers in all domains of computer science and technology to publish high quality, refereed papers. The journal offers articles, survey and review from experts in the field, enhancing insight and understanding of the current trends and state of the art modern technology. Coverage of the journal includes algorithm and computational complexity, distributed and grid computing, computer architecture and high performance, data communication and networks, pattern recognition and image processing, artificial intelligence, cloud computing, VHDL along with emerging domains like Quantum Computing, IoT, Data Sciences, Cognitive Sciences, Vehicular Automation. Subjective regime is not limited to aforementioned areas; Journal policy is to welcome emerging research trends in the general domain of computer science and technology.

## SUBMISSION OF ARTICLES

We invite articles with high quality research for publication in all areas of engineering, science and technology. All the manuscripts submitted for publication are first peer reviewed to make sure they are original, relevant and readable. Manuscripts should be submitted via email only.

To submit manuscripts by email with attach file is strongly encouraged, provided that the text, tables, and figures are included in a single Microsoft Word/Pdf file. Submission guidelines along with official format is available on the following link; www.research.lgu.edu.pk

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence,kindly contact at this address:
IJECI, Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
Email: IJECI@lgu.edu.pk

**LGU International Journal for Electronic Crime Investigation**
Volume 4(4) Year (2020)

## CONTENTS

**LGU International Journal for Electronic Crime Investigation**
Volume 4(4) Year (2020)

# Need to Amend Prevention of Electronic Crime Act 2016 (PECA)

## Editorial

**Kaukab Jamal Zuberi**
**Chief Editor**

Electronic evidence has become an essential tool for solving white and blue collar crimes. However, due to bottle necks in the system, extensive use of digital evidence has yet to be seen in the country. Lack of awareness, quantum of cybercrimes, lack of qualified personnel, lack of awareness in judiciary and legal community, absence of proper procedures to collect digital evidence and presence of sole authority to collect evidence in the hands of one investigating agency are some of Prevention of Electronic Crime Act (PECA) was passed in 2016 and created new offences to prosecute perpetrators using technology to commit crimes. PECA explains the investigation agency and power to investigate as follows:

**Establishment of Investigation Agency:**

The federal Government may establish or designate a law enforcement agency as the investigation agency for the purpose of investigation of offences under this Act. Section 30 of the Act is referred to in this context. "**Power to Investigate**: Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act, provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation team Comprising of an authorized officer of the investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force."

Due to the wide range of new offences introduced in the Prevention of Electronic Crimes Act (PECA) it is almost impossible for an investigation agency to cater all the investigations through one investigative agency. Moreover, it is also not possible for other law enforcement agencies to wait for the bureaucratic procedures of creating a JIT and involving an authorized officer of the investigation agency, authorized under this PECA. At some occasions, timely actions are extremely important to take. For example, searching the house of the alleged member of a terrorist organization, the Anti-Terrorist Force finds a laptop, which is suspected to be used in cyber terrorism, should they wait for the creation of JIT to create images of the hard drive and get vital information out of it through proper digital forensic procedures. It should be noted that the terrorist should be presented in front of the court of law in 24 hours to take the physical remand. Another example can be a house of a suspect who was asking the ransom after kidnapping a child. Should the related police department wait for the creation of JIT before confiscating the mobile phone and start working on the information available to locate the alleged kidnapper.

Moreover, the use of term "dishonest intentions" in PECA creates ambiguity and provides advantage to the accused. Reference is given to the following sections of PECA:

***Section 3:*** "**Unauthorized access to information system or data:**
"Whoever **with dishonest intention** gains unauthorized access to any information system or data shall be punished with imprisonment for a term, which may extend to three months or with fine, which may extend to fifty thousand rupees or with both."

***Section 4:*** **Unauthorized copying or transmission of data:**
"Whoever **with dishonest intention** and without authorization copies or otherwise

transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both."

***Section 5***: **Interference with information system or data:**
**"**Whoever **with dishonest intention** interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with impoundment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

Clauses 6,7,8 are included in clause 10 which describes the offences treated as Cyber Terrorism. Therefore, the prosecutors now have to prove dishonest intention of the accused to prosecute under these sections."

***Section 6:*** "**Unauthorized access to critical infrastructure information system or data:**
**"**Whoever **with dishonest intention** gains unauthorized access to any critical infrastructure information system or data shall be punished wd1 imprisonment which may extend to three years or with fine which may extend to one million rupees or with both."

***Section 7:*** "**Unauthorized copying or transmission of critical infrastructure data:**
**"**Whoever **with dishonest intention** and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both."

***Section 8:*** "**Interference with critical infrastructure information system or data:**
**"**Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical informal ion system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both."

***Section 23:***
"Spoofing: Whoever **with dishonest intention** establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing."

(2) "Whoever commits spooling shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both."

Section 6,7 and 8 are also mentioned in Section 10 which defines Cyber Terrorism.

**National Response for Cyber Crime Center** is the department of Federal Investigation Agency which is responsible for investigating cybercrimes and supporting other law enforcement agencies in solving electronic crimes. Poorly equipped laboratories, lack of trained human resources and neglected standard operating procedures and industry standards have resulted in back log of tens of thousands of cases to be investigated by this department. It is difficult to understand how will they be able to cater the needs of other law enforcement agencies.

There is a dire need to upgrade the laboratories of NR3C, increase number of qualified staff and bring necessary changes in PECA to cover the loopholes (some of them are mentioned here and some are not due to the potential effects on the ongoing investigations/case). Until then, it is expected that the number of unsolved cases will keep on increasing in NR3C and the general public suffering will increase in the hands of cyber criminals.

Aftab Malik *et al.LGU (IJECI)* 2020

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 4 issue 4 Year 2020

# Importance of Prosecution Witnesses in Terrible Crimes of Sexual Violence, Abduction, Abuse, Torture, Rape And Killing Against Innocent Women and Children

[1]Dr Aftab Ahmad Malik Ph.D (England); M.Phil; MSc; LL.B.
Professor, Department of Software Engineering, Lahore Garrison University (LGU),
[2]Mujtaba Asad BS (Hons); MS (Computer Science); MS (Electronics) PhD Scholar,
School of Electronics Information & Electrical Engineering, Shanghai Jiao Tong University Shanghai China
[3]Waqar Azeem BS (Hons); M.Phil (Micro-Electronics Engineering) PhD Scholar
Assistant Professor, Department of Computer Science (LGU), Lahore
dr_aftab_malik@yahoo.com [1], asadmujtaba@sjtu.edu.cn [2], waqar.azeem@lgu.edu.pk [3]

## Abstract:

The cases against innocent women and children are tremendously increasing day by day. The offenders are committing sexual intimidation and harassment accompanied by high degree of torture and killing. The burglars are also observed in such offences with rape, torture and/or killing as modus-operandi. Rape is defined under 'Hadood Laws' in Islamic Jurisprudence and suggests strong punishments. The 'Taazir' sanctions sanctify emerging and contemporary types of criminality. The majority of Islamic penal law's sentences are 'Taazir' in nature. The most popular forms of 'Taazir' include imprisonment, whipping, fines, and the death penalty. According to Islamic jurisprudence, the society must protect its morals, Apart from other factors, this paper focuses on the importance of the prosecution witnesses. The prosecution witnesses are the backbone of criminal case in the court. The criminals and their alias keep on following up the witnesses to prevent and avert the evidence in court; because they know the related information and knowledge about the offence. The paper probes the psychological and psychiatric reasons, why the offenders have abnormal behavior of this type. Therefore, the protection and safe custody of witnesses is of very high importance, particularly in cases of murder and rape. We highlight the ordinary as well as expert witnesses and their role in the cases, regarding proceedings by prosecution. The role of witnesses is of immense importance. This paper presents two case studies to justify that prosecution must built up and collect enough and strong evidence to win the case in court.

**Keywords:** Sexual violence, Abduction, Rape, Burglary, Terrorism.

## 1. Introduction

According to [1], [2] and [3] the practice of murdering and torturing innocent children, including babies, can be dated back to Moses' time. At the time of Muhammad's peace be upon him proclamation of Prophet-hood, the burying of alive innocent girl babies under the age of ten occurred often. Torture, violence, and killing on a large scale are currently happening and being recorded in all subcontinents. A father recently hanged his two-year-old son because the boy was begging

for food. These offences are on the rise, particularly among boys and girls in primary and secondary schools. The "teacher" and his accomplices assaulted a 10-year-old boy multiple times in a "campus." Who will look after the children: the law or the parents? In [3] six relevant case studies have been presented by the authors of this paper.

Despite extrajudicial lynching's and guerilla violence, Pakistani courts have stopped enforcing the hadd sanctions altogether. Just one official amputation took place in Colonel Qaddafi's Libya, in an event against four persons, engaged in robbery in 2003. Nigeria has exercised the same number of hands but no stoning has been reported.

According to [3], a case study of a "religious school" teacher and his accomplice who repeatedly raped a 10-year-old child, with the boy crying blood tears after the attack. In today's world, there are a number of cases involving the raping, beating, molesting, torturing, sexually harming, or murdering of young children, of which the perpetrators use a high level of torture. According to [4], morality and ethics are two terms used interchangeably. Some members of society are becoming enraged, irritated, vengeful, offensive, furious, and reactive in order to exact vengeance, retaliation, and revenge on innocent people, including women and children. Furthermore, we are certain that the exercise and implementation of Islamic law must be implemented in accordance with the law's inherent goals and purpose.

## 2.0 Rape and Zina in Islamic Law

The Zina Ordinance ]5], as established by Pakistan's legislative criminal law, deals with fornication, adultery, and incest, as well as their evidentiary standards and penalties, treating them as similar crimes. If such evidentiary conditions are met. It states the sentences of death by stoning or public flogging for all offences. However, the legal concept of Zina in Pakistan [16], [17] continues to muddy the line between zina and rape. Both zina and "zina by force" are unlawful sexual intercourse, i.e. rape, were specified for the purposes of the ordinance. Clearly, the source of the issue is not theological, but rather a **social behavior** that must be eradicated. As things stand, the abused woman and children bear an unreasonably heavy load. If a woman says that she was assaulted, she should not be forced to validate her point, either to defend her adulterous pregnancy or must report the offence occurred. Her name alone suffices as evidence.

Let us quote the Islamic Model of punishment from Quran Sura Al-Noor verse 2, 4 and 5.

**Quote:**

> "The woman and the man guilty of adultery or fornication, flog each of them with a hundred stripes: Let not compassion move you in their case, in a matter prescribed by Allah, if ye believe in Allah and the Last Day: and let a party of the Believers witness their punishment." (24:2).

**Quote:**

> "And those who launch a charge against chaste women, and produce not four witnesses (to support their allegations), flog them with eighty stripes; and reject their testimony ever after: for such men are wicked transgressors;- Unless they repent thereafter and mend (their conduct); for Allah is Oft-Forgiving, Most Merciful." (24: 4-5).

Hadd is a term used in the Islamic faith to describe punishments that are mandated and fixed by God under Islamic law (shariah). In pre-modern Islam, these penalties were scarcely used. In Islamic law, offences are divided into two categories: those against God and those against man. Hudud offences (apostasy, rebellion against the monarch, stealing, highway robbery, adultery, slander, and consuming alcohol) are punishable by amputation of hands and feet, flogging, and death under Islamic law. The Qur'an mentions a number of hudud offences and, in some cases, prescribes penalties.

The violation of God's prescribed limits for violation, strict punishments having deterrent effects are prescribed by God , are called hudud, or "boundaries". They are linked with punishments stated explicitly in the Quran and explained in hadith. Zina (illegal) is the crime that is punishable by hudud. For example, the *hudud* requirements for *zina* and theft is almost impossible without a confession in court, which could be invalidated by a retraction. Jurists stipulated that the slightest questions or ambiguities should be avoided in order to avoid hudud penalties. There is a hadith of the Prophet May Allah's Peace be him, regarding "shubuhat", shubha. The stricter hudud penalties are intended to discourage people to avoid such offences. According to [18], the offences of accusation of illicit sex against chaste women without four witnesses, hudud punishment is founded in verses of Holy Quran: (9:66), (16:106). (24:2), (24:4) and (24:6).

For example, in Holy Quranic (5:38), the hudud offence of stealing is stated below:

وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا مِّنَ ٱللَّهِ ۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ ﴿٣٨﴾

**Translation:** "As for male and female thieves, cut off their hands for what they have done—a deterrent from Allah. And Allah is Almighty, All-Wise"

## 3.0 Kinds of Witnesses and their Role

A regular witness is one, who has seen or overheard offence firsthand. A regular witness may be the arresting officer or someone who was present at the crime scene. A professional witness is a person who has specialized knowledge of a particular aspect of the crime. A psychiatrist, psychologist, accountant, or other professional may serve as an expert witness. Ordinary witnesses must respond to the lawyers' inquiries and describe what they saw or heard to the court. They don't express their thoughts about what happened.

Expert witnesses offer their views after interpreting the truth of the case. The evidence that witnesses give is made part of proceedings. The testimony is used to decide whether or not the accused committed the offence. When determining whether the accused is guilty or innocent, the judge or jury weighs all of the testimony, including what the witnesses said. The witnesses aid in the clarification of events by informing the judge or jury of what they know about the occurrence of offence.

A witness knows about the case. Government's lawyer and the accused's lawyer will order witnesses to appear in court and tell the judge, and occasionally a jury, for this evidence. Witnesses shall swear or say solemnly that they will testify truthfully in court. Witnesses under the age of 14 or with a learning infirmity will clearly agree to say the truth in such circumstances. The witnesses and the evidence is extremely important, therefore, they must be

protected at any cost. Over the past decade, a variety of factors have raised attention to the involvement of witnesses in criminal trials on a European and international basis.

According to [6], the advent of interest in the role of suspects and witnesses in court cases, as well as the dramatic spike of **terrorist and organized crime**, are perhaps the two most critical causes. All citizens have a civic obligation to provide truthful evidence as witness, if the criminal justice system requires it. Governments, on the other hand, have a responsibility to safeguard witnesses from undue intervention by providing them with security for adequately guaranteeing their safety. Since the successful completion of and step of criminal trials also depend on the assistance of witnesses, providing proper and reasonable security to witnesses will play a serious role in bringing criminals to justice. As a result, the role of the victim is crucial in every current criminal justice system, as adequate forensic evidence is not always available. Furthermore, according to [7], European Union encourages their members to promulgate suitable legislation and measures to guarantee that witnesses may affirm freely and without pressure, while respecting the rights of the defense. The projected actions include practical and legal protective measures.

## 4.0 The Death Penalty

The death penalty is implemented for certain offences in various countries. For a full range of offences, Saudi Arabia has both capital and corporal punishment. **Murder, kidnapping, cocaine abuse, sodomy, armed robbery, apostasy**, and many other crimes are punishable by beheading. Beheading or Crucifixion is a method of execution. In Saudi Arabia, the most common method of execution is beheading with a sword. According to Islamic law, executions must be fast and painless, with the head being separated from the body with a single rapid motion to the back of the neck. Saudi Arabia is a country in the Middle East. Rape in Saudi Arabia serious with punishment by flogging and death, according to Sharia law. In 2019, Saudi Arabia carried out at least 150 killings, eight of which were for rape.

In China, capital punishment is prescribed for some civil offences, murder and cocaine dealing are the most common crimes for which it is used and executions are carried out by lethal injection or gunshot. According to [9], Bangladesh has prescribed death penalty for the offence of rape, as in other six countries but due to an alleged gang rape who sexually raped a woman. In Bangladesh there has been an increase in sexual crime with nearly a thousand cases were reported and registered in 2020, with more than 200 of them were gang rapes. Anyone accused of raping a woman or child will now face "death or life imprisonment" under a new amendment to the country's rape statute. Here are more countries where rapists will face the death penalty.

**Pakistan** is a country in South Asia. Gang rape suspects in Pakistan may be punished to death or life imprisonment under the (PPC) Pakistan Penal Code. After the decision of the case regarding rape of a woman on highway activated protests. Prime Minister of Pakistan stated that the rapists must be chemically castrated or publicly hanged. In this paper, we present the case study of this incident of Robbery with rape.

**India**, three years back by an executive order it was proclaimed that the death penalty for rapists of girls under the age of 12 will be awarded to criminals. This was as result of

reaction to general outcry over a gang of rape allegations, the decision was made. Rapists with previous criminal history had been involved. Some of them were awarded with death penalty under ry's criminal law.

**Iran** is a country in the Middle East. According to Amnesty International, Iran carried out the second largest number of executions in the world in 2020, after China, with at least 250. According to Iran's Islamic Penal Code, 12 of the executions were for rape. **In the United Arab Emirates**, forced Rape with a woman is punishable by death. Compulsion is presumed whether the female victim is under the age of 14 at the time of the offence, according to the statute. In 2019, the UAE did not carry out any executions, but at least 18 people were sentenced to death for offences such as homicide, kidnapping, and armed robbery.

## 5.0 The Death Penalty in China

It is well known that the death in various crimes play important role of deterrence. According to [8], forty two criminal offences in China will be accountable for the death penalty up to the year 2020. Criminals who commit one of these 42 offences in especially heinous conditions can face the death penalty. Anyone who murders a woman or has sexual relations with a child is subject to the country's penal law. The National People's Congress (NPC) elects and can dismiss President of Supreme People.

Photo 1: China's Supreme People Court. Courtesy: [8]

The death sentence in China is prescribed only for heinous offences, according to PRC criminal law. A two-year delay in carrying out execution is permissible in few situations, concurrently with the death penalty. If a local court considers using the death penalty on a criminal, he must appeal to the Supreme People's Court (SPC). Anyone who rapes a woman or has sexual relations with a child under the age of 14 will be sentenced to death, whether the victim survives or is fatally wounded, whether the victim is assaulted in public, or whether the rapist attempts numerous rapes, according to the country's penal code. Amnesty International, the International Labor Organization, and the Death Penalty Database are among the organizations that have provided information about the death penalty.

Table 1: Offences qualified for death penalty. Courtesy: [8]

| There are 42 offences, the punishment is death penalty in China. A few are given in this Table | | | |
|---|---|---|---|
| **Rape** | **Trafficking women & children** | **Kidnapping** | **Robbery** |
| Theft, snatching of guns, | Stealing, spying, | Theft of weapons, | Robbery of guns, |
| Arson | **Betrayal of Country** | Bribery | Explosion |

## 6.0 Element of Deterrence of Death Penalty Imposed Publicly

The statistics show that death penalty imposed publically has a great deterrent impact in reducing the crime rate in China particularly in countries like Saudi Arabia. In Iran and Bangladesh public hanging has been exercised. According to [15], the principle of deterrent is important dimension of a sanction scheme is

the likelihood of death, if convicted of a capital punishment qualifying murder. Many trials have been conducted during the last five decades to see whether the death penalty has any impact on murder rates. Researchers have come to highly disparate, often conflicting conclusions. Some reports have shown that the possibility of capital punishment deters killings and saves many lives; others have found that executions increase homicides; and even others have found that executions have little effect on murder rates. Researchers, supporters, and lawmakers weigh in on the scientific findings and statistics.

In light of this, the National Research Council's study Deterrence and the Death Penalty examines whether the existing data offers a scientific foundation for determining whether and how the death penalty impacts murder rates. A new report by the Committee on Law and Justice concluded that the available research on the effects of capital punishment on murder rates is inadequate to assess if the death penalty increases, decreases, or has little effect on these rates. The key question is whether capital punishment is less or more effective as a deterrent than other alternatives, such as life without the possibility of parole.

## 7.0 Psychiatry Based Analysis on Why Rape and Sexual Violence?

Why women and children are abused and tortured? It is due to poverty, a lag in young male marriages, unemployment, and the lack of any legal deterrent force absence of fear of God, which is the most powerful source of deterrent and avoidance, projection of naked and obscene content and footage on social media, films; anti-social elements' use of drugs. The other reason is that the criminals suffer from psychological issues and disabilities. The reasons for committing the rape may be due **bipolar disorder, severe psychosis, depression, serious organic brain disorders or learning disability**. The recent increase in sexual violence against women as rape perpetrators have mental health and psychosocial causes. But they sustain, and continue to commit the crime. Psychiatrists can help criminal justice departments manage this scourge in a positive and educational way. According to [10], a variety of preventive programs have emerged in reply to the terrifyingly high prevalence and harmful effects of child sexual misuse. In this article, both overt and indirect primary and secondary intervention are discussed. Although there are many innovative and engaging preventive projects for kids, scientific validation has lagged behind their actual creation and execution. Our investigation has revealed that further adult-oriented policy implementation and assessment is wanted to help in child sexual exploitation. A number of studies issue must be addressed.

According to [11], in recent years, treatment of sexual disorders is being focused. Sexual dysfunctions, and gender identity disorders are distinct. “Hyper active-sexual desire disorder” and other sexual desire disorders should be included in the sexual dysfunction dis orders. There should be a separate category for paraphilias "with hyper-sexuality" and "without hyper-sexuality." Despite functional neuro-anatomical and neoro-pharmcological research, there is still a lack of complete understanding of the neurobiology of sexual disorders.

According to [12], there has been a surge of research in the treatment of sexual illnesses. Sexual dysfunctions, paraphilia’s, and gender identity disorders are all categorized as sexual

disorders in the DSM-IV. Non-deviant or non-paraphillic sexual dysfunctions exist. "Hyperactive sexual appetite disorder" should be included under sexual desire disorders in the list of sexual dysfunction disorders. There can also be a distinction between paraphilias "with hyper-sexuality" and "without hyper-sexuality." While functional neuro-anatomy and neoro-pharmcological studies have shown the neurotransmitters, receptors, and hormones involved in sexual disorders, there is still a lack of knowledge of the neurobiology of sexual disorders.

According to [13], there exist a connection between Psycho disease and symptoms of sex-offending tendency in men with schizophrenia, which are common. An experiment was conducted by the authors of [13] with eighty four males in sample and restricted medical order having schizophrenia, in 1997, with an index conviction for a contact sex offence against a woman Their record were searched from Home Office database. It was found that eighty men were delusional at the time of their offences, and half of them suffered visions or hallucinations linked to the offences. Only eighteen men had a specific psychotic or illness of “hallucinatory motor”, but majority of men did.

According to [14[, the effectiveness of recovery services in rehabilitating rapists has yet to be determined empirically. Care can be based on a scientific view of rape and abusers, as well as evidence-based experience of treatment outcomes for rapists, according to a scientist-practitioner viewpoint.

## 8.0 Case Study 1:

Imran Ali, a Kasur native, was accused of being involved in at least nine rape-cum-murder of minors, including Zainab's, which he admitted to during the investigation into her murder. Zainab's rape and murder earlier in 2020, caused indignation and demonstrations around the country after the six-year-old girl was discovered dead in a garbage heap in Kasur after going missing. Over the course of a year, Zainab's case was the twelfth such incident to occur within a 10-kilometer radius of the district. The court has reached a decision in five of the seven rape and murder lawsuits filed against Imran. Imran Ali, the man accused of terrorism, was sentenced to death by an Anti-Terrorism Court (ATC).

In Zainab's case, the prosecution presented all of the testimonies, oral proof, computer forensic evidence, and the accused's confessional declaration very tactfully and skilfully in logical sequence. The ATC had sentenced him to death on four counts, as well as a life sentence, a seven-year prison sentence, and Rs 4.1 million fine. The four men were sentenced to death for abduction, rapping, and killing Zainab, as well as for committing a terrorist attack under the provisions of “Section 7 of (ATA) Anti-Terrorism Act”. Imran Ali has been sentenced to 21 counts of capital murder, three life terms, and a total of 23 years in prison. The court has also imposed a Rs 2.5 million fine on him, which is less than the amount he owes.

Only solid facts gathered by police and submitted in court by the prosecution was able to bring Zainab to justice. As a result of the horrific nature of the murder, riots erupted in Kasur almost immediately. Ali's appeal against his death penalty for the rape and murder of Zainab was dismissed by the Supreme Court of Pakistan due to solid facts, recalling that the appellant had confessed to committing similar crimes with eight other minor victims and that "in that backdrop, he did not deserve any

sympathy in the matter of his punishments."

### 8.1 Case Study 2: Motorway Gang-Rape Case Where Prosecution Presented 53 Witnesses

The purpose of this case study is to prove that proper procurement of witnesses and presentation in the court of Law is extremely important. The prosecution had very successful contested each and every evidence of 53 witnesses correctly, appropriately, properly, suitably and in befitting manner and legal procedure. This approach also is beneficial to the prosecution case.

A lady travelling in her car with children in September 2020, vehicle stopped near Gujjarpura due to lack of petrol. She dialed a relative's number and texted him, her place on the highway. When the relative arrived, he observed that the woman had been distressed and there were blood stains all over her clothing. Her vehicle's windows were also broken and shattered.

The victim told investigators that she and her children were waiting for a parent to pick them up when she was assaulted by two armed men. One of them used stick to attack her, while the other took them detained at gunpoint, insulted, kidnapped her with the children and gang-raped her in a nearby forested location. The heinous crime sparked a nationwide outcry. The crime attracted widespread outrage around the country, with demonstrators calling for the perpetrators to be publicly hanged, while others marched through the streets urging judicial changes to protect women and children. The shocking event sparked a discussion on mass and social media about behavioral patterns and the troubling increase in cases of sexual assault as well as the law enforcement system's failure to provide people with protection, as even driving on a highway has become dangerous.

Abid Malhi and Shafqat Hussain, the defendants, were said to have seen the woman waiting for help in her vehicle, according to prosecutors. The assailants smashed a window and pulled her outside, where they raped her at gunpoint in front of her frightened children, despite the fact that she had locked the car doors. They later left her stranded after robbing her of valuables including Rs 100,000 cash, two items of gold jewelry, a ring, registration card and papers of car along with three ATM cards. The rape victim's unwillingness to file a police report demonstrates his distrust of the procedure. They were apprehended afterward due to matching of DNA samples, obtained from the crime scene. The men were later detained by police and charged.

## Court Proceedings

In December 2020, Pakistan promulgated new rape laws. Special courts were set up for hearing such cases.

The prosecution and the investigator were asked to be active to peruse such matters. The criminals Abid Malhi and Ali depended on state defense layers. The investigators had identified the criminal Abid Malhi as main accused. The request of the prosecution to record the evidence of the minor children of the victim was turned down by court. However, the children appeared before the court. The judge asked them simple question like: “which school you study?” and “In which class you are?”. The children did not reply and said they don’t know.

The prosecution very successfully pleaded and presented all the 53 witnesses. The defense council pleaded that criminals are not guilty but could not establish. Then the Judge recorded and cross-examined statements of

around 35 prosecution witnesses.

## Judgment

The Judgment was written under the provisions of Pakistan Penal Code and Anti-Terrorist Act (ATA).against the criminals Abid Ali and Shafqat Ali on the allegations of Abduction, mischief, Rape and Robbery, which is summarized below:

| Charges criminals | Award of Punishment to both |
|---|---|
| Abduction | Life imprisonment |
| Robbery | 14 years plus a fine of Rs 200,000 |
| Rape | Death sentence |
| Mischief | 5 years imprisonment plus Rs 50,000 fine |
| | Payment of Daman to victim by both convicts: Rs 500,000/- |

**Quote:**

> "The offence of rape is heinous offence and when it is committed in the eye sight of children of the victim, heinousness further magnified and which is shocking for general public as well so such accused persons should be dealt with iron hand," the judge wrote in a verdict. The court noticed that both accused took victim from the vehicle forcibly and brought her down in a jungle; "which reflect common intention of both the accused so both the accused persons committed offence u/s 376(ii) PPC [Pakistan Penal Code] in furtherance of their common intention, thus both the accused namely, Abid Ali s/o Akbar Ali and Shafqat Ali and Bagga s/o Allah Ditta are convicted and punished u/s 376(ii) PPC to Death".
> Unquote.

The judgment said that convicts be hanged until; but sentences should not be executed till its confirmation by the Lahore High Court. Besides confiscating their properties, the court also awarded them life sentences over kidnapping and adducting charges. The court also imposed Rs 200,000 fine each and also awarded 14 years imprisonment to both accused under Section 392 of PPC for robbery. The court awarded five years imprisonment to both accused under Section 440 of PPC for mischief, besides imposing Rs 50,000 fine.

"It has been established on record that during instant occurrence victim received injuries which comes within the ambit of Jurh Ghayr Jaifah Damiyah, thus both the accused persons are convicted and punished u/s 337-F1 and they are directed to pay Daman Rs.50,000/- each to the victim" . All the sentences shall run concurrently and benefit of Section 382-B CrPC shall be given to each convict, it added.

## Recommendations:

- Cultural warfare, poverty, unemployment and economic deprivation have a negative impact on humanitarian ideals, morality and ethical expectations. Terrorist attacks are being committed by certain criminals against innocent women and children and civilians, as discussed in the case study. Today strict laws are needed. The death penalty, according to public demand, must be exercised publically in cases of horrible, awful, dreadful, scandalous, and wicked offences committed against innocent women and children.

- Owing to non-reporting of incidents, the real figures are exceptionally high. Domestic child and women labor must

be prohibited by federal authorities.

- Abuse and inhumane torture disproportionately affect girls and boys under the age of 15. Village women take their daughters to cities to work as maids on a monthly or advance payment basis, and they don't care what happens to them afterwards. More action is needed by the state to protect children from neglect and death.

- Most challenges occur when fighting lawsuits in a court of law due to naïve evidence. The executive and the police-prosecution division are two essential parts of the police force. The executive reviews and sends the matter to the district attorney for legal advice, who then forwards and appeals the case as a public lawyer before a court of justice, where the state is a party in criminal trials.

- The argument to remember is that our legal system must be sufficiently strong to deal with all complex circumstances that arise from the application of law. For crimes such as kidnapping, molestation, rape, sodomy, incest, and murder, the solid proof is required for the case to be heard in court presented by the prosecution.

- We advocate enacting a strict regulatory system to shield women and children from acts of torture, rape, violence, and murder. Our greatest interest, right of way, and first priority must be the safety of women and children.

- Abuser organizations and gangs must be apprehended, taken into custody, questioned, and, if necessary, held under the rules to defend our women and children from both internal and external forces of darkness. We must protect women and children from cultural warfare attacks and the dangers posed by abuser gangs, untrustworthy families, and "boy-friend-culture" with poor habits, particularly those who use drugs.

- The rapists must be chemically castrated or publicly executed.

- Using information technology, roaming information stored on the telephone and service provider end, the addresses of the travelling offenders can also be identified. Forensic data may be retrieved from mobile messages. Other information on the offenders' mobile phones and laptops, such as images, videos, SD cards, and call logs, can be easily traced.

## Conclusions

We conclude that proper r procurement of witnesses and presentation in the court of Law is extremely important. In this way as seen in both case studies above the prosecution can successful contest each case and every evidence, if presented the witnesses correctly, appropriately, properly, suitably and in befitting manner and in conformity with legal procedure. This approach also is beneficial to the prosecution in all cases. The death penalty, according to public demand, must be exercised publically in cases of horrible, awful, dreadful, rape, scandalous, and wicked offences committed against innocent women and children.The state of Pakistan must seriously restrain, curb, control, limit or curtail the occurrences of heinous offences and violence against innocent women and children in spite of the availability of various enactments/legal

instruments in the field including amended PPC and ATA.

## Acknowledgement:

The authors acknowledge the valuable guidance of Mr Kaukab Jamal Zuberi, the Chief Editor and Director DFRSC, Lahore Garrison University, extended during this research work.

## References:

[1]: Dr Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem (2019), "Electronic Devices to Investigate Offences of Torturing, Abusing, Molesting, Assaulting or Killing the Innocent Children, LGU International Journal for Electronic Crime Investigation Vol. 3 Issue 2, April - June 2019.

[2]: Dr Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem (2021), "Combating With the fast growing Epidemic of Child Abuse, Torturing and Killing Seems a Difficult Task", LGU International Journal for Electronic Crime Investigation.

[3]: Dr Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2020) ," Promulgate Strong legal framework for child protection against offences of torturing, abusing or killing"; International Journal for Electronic Crimes Investigation"(IJECI) Published in Volume 4 issue 2, April-June 2020 ; PP 1-10.

[4]: Dr Aftab Ahmad Malik, "Tafakkar-e-Rasool", Book on Holy life of Prophet Muhammad Peace be Upon him; Published by Al-Kausar Publications , Lahore.

[5]: The Offence of Zina (Enforcement Of Hudood) Ordinance, 1979. www.pakistani.org › Pakistan › zia_po_1979 › ord7_1979

[6]: Felföldi Enikö (2006), "The rising importance on the protection of witnesses in the European Union" Dans Revue internationale de droit penal 2006/1-2 (Vol. 77), pages 313 à 322 https://www.cairn.info/revue-internationale-de-droit-penal-2006-1- page- 313.htm

[7]: The Role of Witness, https://educaloi.qc.ca/en/capsules/the-role-of-witnesses/

[8]: Yuan Yanchao (2020),"How Many Crimes Are Punishable by Death in China？", Contributors: CJO Staff Contributors Team; https://www.chinajusticeobserver.com/a/how-many-crimes-are-punishable-by-death-in-china

[9]: Naimul Karim (2020),"FACTBOX - From Bangladesh to Iran, countries where rape carries the death penalty", Naimul Karim | @naimonthefield | Thomson Reuters Foundation.

[10]: Cindy L.Miller-Perrin (1988), "The child sexual abuse prevention movement: A critical analysis of primary and secondary approaches", Clinical Psychology Review; Volume 8, Issue 3, 1988, Pages 313-329

[11]: John MW Bradford (2001), "The Neurobiology, Neuropharmacology, and Pharmacological Treatment of the Paraphilias and Compulsive Sexual Behavior", Canadian Journal of Psychi-

atry, PubMed https://doi.org/10.1177/070674370104600104

[12] J M Bradford (2001), "The neurobiology, neuropharmacology, and pharmacological treatment of the paraphilia's and compulsive sexual behavior" Can J Psychiatry, 2001 Feb;46(1):26-34; PMID: 11221487 ; DOI: 10.1177/070674370104600104

[13] A D Smith , P J Taylor" Relationship of illness and psychotic symptoms to offending" PMID: 10448448 , DOI: 10.1192/bjp.174.3.233

[14] Theresa A Gannon , Rachael M Collie, Tony Ward, Jo Thakker, "Rape: psychopathology, theory and treatment, PMID: 18378054, DOI: 10.1016/j.cpr.2008.02.005

[15] "Determining the Deterrent Effect of Capital Punishment", www.nap.edu https://www.nap.edu/read/13363/5

[16] Zina, Rape and Islamic Law: An Islamic Legal Analysis of the Rape Laws in Pakistan. A Position Paper by KARAMAH: Muslim Women Lawyers for Human Rights

[17] A. Quraishi (1999), "Her honour: an Islamic critique of the rape provisions in Pakistan's ordinance on zina," Islamic studies, Vol. 38, No. 3, pp. 403–431 (via JSTOR)

[18] The crime of "accusation of illicit sex against chaste women without four witnesses" and a hudud punishment is based on Quranic verses 24:2, 24:4, 24:6, 9:66 and 16:106

[19] https://news.sky.com/story/pakistan-pair-sentenced-to-death-for-raping-woman-in-front-of-children-12252317

[20] https://tribune.com.pk/story/2290463/atc-awards-death-sentences-to-motorway-gang-rape-accused

[21] https://www.thenews.com.pk/print/806516-verdict-in-motorway-gang-rape-case-tomorrow

Marium *et al.LGU (IJECI) 2020*

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 4 issue 4 Year 2020

# Cyberbullying Brutally Affecting Society

**Syeda Marium Nizami**
mariyum002@yahoo.com
LCWU

## Abstract:

This article provides in-depth information about Cyber Bullying. Cyber bullying equally affects lives of individuals negatively. The victims suffered from bullying by friends, close relatives and people close to them. The continuous act of Cyber bullying creates immense pressure which may lead the victims to commit suicide. There is an alarming rate of cyber bullying victims in the younger population. The paper suggests strategies to decrease cyber bullying in society, in general, and educational institutions in particular.

**Keywords**: Cybercrime, Cyber bullying; Internet; Prevention; Students, strangers, suicides, psychopaths.

## Introduction to Cyberbullying

Bullying isn't a new concept, but the universal adoption of new communications technologies that has caused bullying behavior to move to cyberspace, this phenomenon is known as "Cyberbullying." Because of its increased estimated frequency and the fact that it has been suspected as a main factor in a number of teen suicides, Cyberbullying is becoming a growing cause of worry for parents, police, educators, and the general public. Bullying is categorized as the widespread abuse of power by unreasonable and recurring actions designed to annoy or injure another person. It can have a direct or indirect effect like physical and verbal teasing. Bullying has become more of a challenge for teenagers and educators, particularly with the increased use of digital technologies that allow for quick and widespread communication. Bullying has previously been connected with educational environments; however, this is no longer true, as emerging technologies allow sexual abuse to happen outside of school hours and at any moment during the day. [1]

## Another Way of Defining Cyberbullying

There is currently no generally recognized way of defining Cyberbullying, but many of the concepts studied share similar elements. The Senate Standing Committee on Human Rights review, Cyberbullying Hurts, Respect for Rights in the Digital Age , recognizes the difficulty in reaching agreement on a consistent definition of Cyberbullying, owing to a lack of shared idea of what constitutes this practice. [2] The Analysis found support for

the argument that Cyberbullying is a form of conventional bullying, claiming that Cyberbullying involves actions meant to harm, ridicule, assault, or abuse the victims. Cyberbullying occurs in many ways, that includes sending offensive and intimidating messages via email, text messaging, and phone calls, as well as sharing such messages in discussion groups, "bash boards," and some other social media websites. [3] The digital sharing or electronic dissemination of humiliating pictures or videos is yet another common method of Cyberbullying. It may also mean making websites insulting, tormenting, and bullying the alleged target or victims. Cyber bullies are also using certain platforms to set up opinion polls or voter rolls, enabling site users to vote on subjects like who is the "dumbest" or "ugliest" student in class. [4] According to a new report, one out of every three high school students has experienced bullying or Cyberbullying in some way. 8th footnote According to Statistics Canada's Self-reported Internet Victimization in Canada, 2009 Footnote 9 (based on the General Social Survey (GSS) on Victimization), 7% of Web users aged 18 and up have been victims of Cyberbullying at some point in their lives. Violent or offensive e-mails or text messages were the most common type of Cyberbullying, as recorded by nearly three-quarters (73%) of Cyberbullying victims, followed by negative comments by more than half (55%) of survivors. In the study, 8% of teenagers had their identities stolen by someone who then sent them offensive e-mails. [5] Messaging and networking sites web users were nearly three times more likely to become victims of Cyberbullying than someone who did not ever use sites. A stranger cyber bullied the number of people between the ages of 25. (49 percent). Bullying was most common among people aged 15 to 24, who were harassed by a peer, student, or colleague (64 percent). Males are more likely than females to be intimidated by a stranger (46% vs. 34%), and female are also more likely than males to be bullied by a colleague or workmate (13 percent versus 6 percent).[6]

Adult respondents were also asked if any of their kids or youth (ages 8 to 17) had been victims of abuse or child luring in their home. [7] According to the findings, 9 percent of adults living in a household with a child were aware of a case of Cyberbullying involving at most one of their kids. Of these adults, 74 percent responded that the Cyberbullying was in the form of violent or harsh e-mails or messages. [8] This was followed by terrible comments sent by e-mail or messaging or posted on a website (72 percent ), and having someone use the child's identity to send threatening messages (16 percent ). The percentage of parents said the kids were harassed by someone they met, such as a colleague (40%), a relative (20%), or an associate (11%) rather than an outsider (21 percent ). [9]

Furthermore, it is discovered that only a small percentage of Cyberbullying cases were criminally prosecuted (7 percent of adults and 14 percent of children). "Since Cyberbullying is not always relevant to the investigation and therefore does not require prosecution to police, other steps may be more effective," the authors write. Survivors were more likely to block messages from the source (60 percent), leave the site (51 percent), or complain the circumstance to their Internet or e-mail network operator, according to the data (21 percent ). [10] Other explanations for not disclosing Cyberbullying, according to statements provided to the Standing Senate Committee, include fear of confrontation, inappropriate responses in the past, and risk of losing access to their data. It's harder to form

broad conclusions about the occurrence of Cyberbullying because evidence suggests that rates differ widely based on a number of reasons. Nonetheless, recent Comparative research on the existence and incidence of Cyberbullying show that Cyberbullying is a common occurrence that mostly affects teenagers but also grown up. [11]

Youth who have a disorder, are overweight, are members of ethnic minority groups, and those who identify as, or are considered to be, lesbian, homosexual, bisexual, or transgendered are all at risk of being targeted, according to the study. Cyberbullying is especially harmful because it can reach a large number of people in a short amount of time, anonymously or by manipulation, and it can last forever online. Teenagers and adolescents who are victims of Cyberbullying are more likely to suffer mental, psychological and emotional damage, such as chronic stress, academic difficulties, and acting out problems (e.g., weapon carrying). [12] Victims of Cyberbullying may feel powerless, which may lead to youth crime and suicidal thoughts. These consequences are believed to be caused by the significant role of digital communications, the large population reached by digital communications, and cyberspace's indestructibility [13]

## What is Cyber-Bullying

Cyber harassment is described as when the Internet, mobile phones, or other devices are used to send or post text or photos meant to intimidate or disgrace other individual" by certain definitions. [14]“A condition in which a teenager is regularly ‘brutalized, harassed, threatened, mocked, humiliated, or violated' by another teenager using messaging apps, e-mail, text messaging, or any other types of electronic new technologies,”. Since cyber-stalking may refer to bullying between adults through the internet or mobile phones, the last meaning only applies to teenagers or youngsters.

A cyber harassment scenario can be as easy as sending e-mails to those who have requested that you lose contact with them, but it can also be very severe when it involves harassment, sexual assault, or the development of a website where that individual is mocked. Psychopaths may post confidential info about their offenders on websites or forums, or even appear to be anyone else in addition to publishing derogatory or humiliating material in the victim's name. The majority of bullies use a similar strategy, sending offensive messages to their victims or calling them derogatory names.

## Who is a Cyber-Bully

A cyber harassment is typically a victim of his community, where he is manipulated in a variety of ways, including emotionally and psychologically, and may even be cyber harassed. However, it's possible that they're just lonely or corrupt enough to make someone else's life a shambles. Many times, cyber harassed operate in communities although it makes them feel better, but they may not enjoy their behavior indulgently. Their biggest issue is that they are unable to leave their team because they feel insecure and are afraid of being cyber harassed themselves. Studies have identified that oppressors are often more frustrated than their hostages. What should bother everybody is that when cyber-bullies send intimidating and flame e-mails to their victims, they get a false sense of gratification because they are amusing themselves. The primary goal of cyber bullies, as well as conventional bullies, is to gain control. They want to be in control of any condition. They

want to rule over others and marginalize them.

## Effects of Cyber-Bullying

Cyber Harassment exemplifies the technology's ugliness. Cyberbully survivors may become distressed and, in the worst-case scenario, attempt suicide. As a result, it can be see how the internet is disruptive and unfamiliar to the majority of people, capable of “hurting” them if they are unaware of the internet in general. Cyber Harassment has a number of detrimental consequences for individuals and communities. It usually begins with the survivor being perplexed and humiliated because an individual or a group of people has singled them out and humiliated them for no other reason than to be cruel. Most people would wonder why they are being bullied, but maybe even cyber-bullies have no idea. They gradually develop feelings of fear or isolation, as well as apprehension about leaving their home or attending school. If a victim is bullied on a regular basis, his grades will suffer, and he may even exhibit paranoid symptoms, finding it challenging for him to interact with peers or meet new people. Mental illness is one of the consequences of cyberbullying, and the term "symptoms" is used because it appears that cyberbullying has become a "sickness" in our environment. The survivor feels lost because they don't know who to turn to for assistance. Of course, in severe cases of relentless bullying, suicide can be a factor. Cyberbullying should be prohibited, but the question is how to do so.

## Proper Individual Reaction

The United States of America is thought to be more worried with cyber-bullying because of the large percentage of their people that is impacted and the comparatively large number of cases registered, prompting them to pass legislation against it.The advice to an average person would be to just Ignore the bully, don't take him seriously, don't answer to him, and ignore him again if he shows up at your place. It is recommended to tell advisor or parents about it so that they can assist. If the victum does not react to cyber-bullies, it is likely that they will become discouraged and move on to the next victim. Nonetheless, these recommendations would only assist an individual in avoiding cyber-bullying. Furthermore, while cyberbullying may not go away, it is a good place to start for indiscriminate harassment.

Significance of Cyber-Bullying

How real is cyberbullying as a threat. Adults generally agree that cyberbullying, along with traditional bullying, is to blame for much of the psychological, depression, and anxiety issues that children face, since this is the situation that has the most impact on them. Many teens, on the other hand, disagree with this assertion; they believe that cyber-bullying is less of a concern because nothing is “genuine” on the internet, and what is said or performed should not be adjusted to reflect as much. Teens, think that they know advancement of technology better than adults, and thus are not duped by the media, whose job is to report any situation in the most sensational way possible. However, this does not justify the rising number of suicides among teenagers. Anyone who claims to be oppressed in the digital environment knows very little about how to defend themselves, even though they are. Authentically, the internet does not always reveal its true "face," and cyber-bullying is far from the only thing to be concerned about. The internet is full of mysterious traps and contradictions that can lead someone astray. Cyberbullying is a major problem that is alarming our culture on a daily basis. Cyberbullying isn't the last aspect that should be concerned with. People must be trained with

the ways of how to avoid cyberbulling.

## Real Life Incidents of Cyber Bulling

Megan Meier, a 13-year-old girl from Missouri, committed suicide in her bedroom in 2008, surprising most people in the United States into knowing what cyber-bullying is. Megan died as a result of excessive stress brought on by persistent and cruel cyber-bullying, according to investigators Adults such as Lori Drews, the father of Megan's friend with whom she had a fight, and an 18-year-old officer who worked for M. Drews claimed to be a mystery man in Megan's neighbourhood and started a relationship with her via Myspace (a social networking site). Megan had been duped into believing she had an increasing relationship with the "kid" by the party. Megan lacked the emotional strength to cope with the embarrassment of being ridiculed after the hoax was exposed, so she committed suicide. Since Missouri did not have any legislation against cyber-bullying at the time, none of the members of the family could be prosecuted. In Massachusetts, another tragedy occurred. Phoebe Prince, a 15-year-old Irish migrant, was abused at school, on the internet, and on her computer. She declined to change her Facebook settings or cell phone number for threat of damaging her few friends. Even worse, her perception of herself as a "loser" drove her to commit suicide.

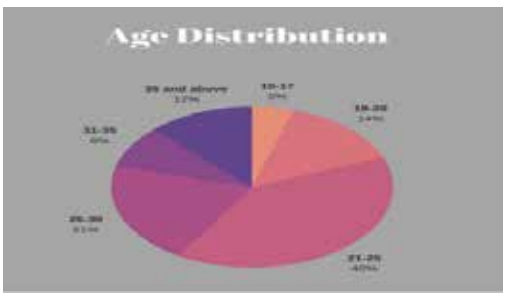


Figure 1 Age Distribution Pie Chart

Fig 1 shows a pie chart of age distribution that what is the percentage of which age group that is being affected by Cyberbullying

The figures are as surprising as the events themselves. According to a 2008 cyber-bullying study survey of 2.000 middle-school students, approximately 43% of them have been victims of cases that can be classified as cyber-bullying: “Receiving an instant message that offended them (15.8%)”“Obtaining something written on their MySpace that irritated them (14.1%).” “Even more concerning, a survey of 1,247 young people aged 14 to 24 conducted by AM/MTV in September 2009 found that”: “50 percent of youngsters in this age group have encountered digitally abusive behaviour, with older teens aged 18-24 (52 percent vs. 47 percent ) and females more likely to be targeted (53 percent vs. 42 percent )” “On social networking sites, 45 percent of young people claim they see people being rude to each other.”[15]

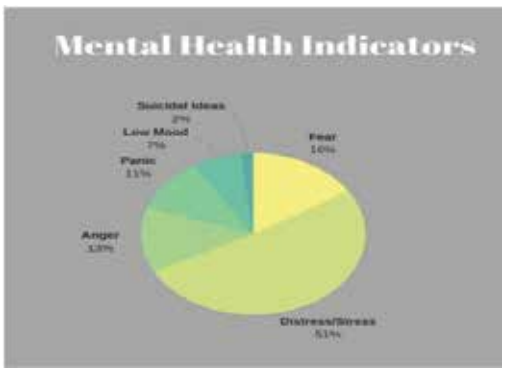


Fig 2 shows the pie chart containing the percentage of victim’s mental health

## The Relationship with Traditional Bullying

“Sticks and stones can break your bones, but names will never harm you,” as the saying

goes. Personally, I disagree with that statement. Despite the fact that Cyberbullying is less physical than conventional forms of bullying, it has much more damaging and long-term consequences for victims. It is very simple to gain access to a machine and destroy someone's mental health. People overlook the fact that anyone, even a young, physically vulnerable child who has been a victim of conventional bullying, may be a bully online. The difference is that someone is now in a position to do much more harm than a large force. “The internet is a sinister, silent enemy: you simply don't know where to start to tattle,” Emily Moor, a British bullying survivor, said. But, as faceless as a machine can be, it is just as dangerous as a human bully, if not more so, because the audience reading these heinous messages can be massive. While it is true that if you are bullied at school, you can simply go home and stop it, you have nowhere to go if you are cyber bullied..

## Laws Against Cyber-Bullying

It is already widely acknowledged that the presence of false identities or identities with back stories makes it difficult to identify the perpetrator. Law makers are attempting to pass new cyber-bullying law since it seems that there are currently no standard laws in place that tackle the issues. They want to combat cyberbullying by enacting legislation that designates the act of harassment as bullying. Nonetheless, it is difficult to find a wealth of knowledge on laws prohibiting secret identities or false accounts, with the exception of states such as Texas and Georgia, which have enacted laws prohibiting people from posing as anyone else on the internet. What's more, people who create fake profiles on social media platforms can face charges for their antisocial conduct. [16]

Legislation aimed at punishing cyber-bullying and digital bullying has been passed in a number of US states, including New York, Missouri, Rhode Island, and Maryland. In 2007, at least seven states enacted legislation prohibiting cyberbullying. For example, the city of Dardenne Prairie in Springfield, Missouri, has made online bullying a misdemeanour. Furthermore, in 2008, state lawmakers in Jefferson City, Missouri, gave final approval to a bill making cyber-bullying illegal. Supporters agree that this bill would cover bullying that occurs by computers, text messages, and other mobile devices. The first bill dealing specifically with cyber-bullying was passed in August 2008 by the California state legislature. The bill was dubbed "Assembly Bill 86 2008," and the aim was to add provisions to the School/Law Enforcement Partnership Act that dealt with bullying conducted through an electronic communication device or system. To that end, a concept of electronic communication was added to the School/Law Enforcement Partnership Act. Even if many schools are now able to confront cyberbullying as a result of the following changes, I will hold the following details in the Laws Against Cyber-Bullying portion.

In Arkansas, a law was passed in 2007 that allowed school officials to deal with cyber bullies even if the bullying did not occur or begin on school grounds. Following the passage of the legislation, school administrators were given more leeway in punishing bullies.

Several laws have been passed in Iowa that require schools to enact anti-cyberbullying policies that include bullying that occurs in the classroom, on school property, or at any school event or activity supported by the school.

New Jersey has always had tough anti-bullying regulations, but there were no laws in place that specifically addressed cyber-bullying until 2007. Once again, the legislation empowers school officials to discipline students who engage in bullying behaviour against their peers.

Idaho lawmakers passed a law in 2006 that authorised school employees, especially officials, to suspend students who harassed other students using a computer or other electronic device.

They wanted to investigate cyber-bullying in greater depth and broadened the definition at Oregon State University.

Recently, the governor of Rhode Island attempted to pass a bill that would prosecute cyber-bullying perpetrators for violating the state's rules.

Vermont already had stringent anti-bullying and anti-cyber-bullying rules, but lawmakers recently imposed a $500 fine for those who are abusive to those on the internet. Vermont is regarded as one of the states with the most stringent anti-bullying laws.

## Laws Against Cyber-Crime in Pakistan

In recent years, cyberbullying has become a big issue in Pakistan. Thousands of young people have become used to receiving unsolicited slanderous, offensive, and derogatory messages and comments on their social media pages. According to a survey conducted by the Express Tribune in 2013, 75 percent of online consumers were men, indicating male dominance on the Internet. Unfortunately, young women in Pakistan are subjected to online abuse by men, and this problem has gotten worse in recent years as a result of increased social media use. Men's bigotry and discrimination have been perpetrated against Pakistani women who have been oppressed on the Internet. Online abuse is a problem that can be seen in both developing and developed countries. A mushroom growth of online abuse has tarnished the image of many young people in a country like ours, where technology invades earlier than its due SOPs. Women are psychologically depressed as a result of being intimidated, maligned, and blackmailed by fake accounts. If cyber criminals were not curtailed by legislation, the future of social media in Pakistan will be bleak. In Pakistan, the participation of a few genuine private individuals in leading this cause to safeguard women's integrity and privacy is a landmark moment.

## The Prevention of Electronic Crimes Act – PECA)

Parliament passed a bill (The Prevention of Electronic Crimes Act – PECA) in 2016 that aided in bringing cyber criminals under the jurisdiction of the law. Anousha Rehman Khan (a lawyer and minister of state for information technology and telecommunications) has clarified on several occasions how a large number of lives have been lost as a result of the abuse of social media and how important it is to prevent this from happening again. Regardless of the fact that the legislation has been passed, there is no public knowledge of it. Few private companies acknowledged the need to protect and protect people (especially women) from cyber bullying.

## Digital Rights Foundation (DRF)

The Digital Rights Foundation (DRF) is one such agency that operates to increase

awareness, particularly in women, about the importance of protecting their social media accounts and reporting legitimate online abuse reports. DRF published a study in 2016 to collect data on women who were abused online. This study was conducted in 17 of Pakistan's major universities throughout the country, in all of the country's provinces. The results were shocking, with 34% of respondent (all women) admitting to having experienced online harassment and 55% admitting to knowing about other women being harassed online. When asked how effective the FIA was in dealing with online abuse complaints, 47 percent said it was immensely beneficial and also that their reports were properly examined. However, 53% believe that the reporting process should be more sophisticated and precise because it is ineffective. Surprisingly, 72 percent of educated women were unaware that there was a law against online abuse.

The Hamara Internet (translates as "Our Internet") project was completed successfully, and the "Measuring Pakistani Women's Experience of Online Violence" study was used to launch the Cyber Harassment Helpline. Our research aimed to debunk the misconception that digital rights are a niche issue; according to the Hamara Internet campaign, 79 percent of young women use digital technology. The use of these devices is based on gender and motivated by the user's identity. Adult women are more likely than men to consciously their personality traits and to be harassed online. This makes them, as well as other groups in Pakistan such as religious and ethnic minorities and liberals, more vulnerable in online spaces. When it comes to dealing with online abuse in personal cases, DRF has noticed a significant difference. Established law enforcement agencies coping with online abuse have a low level of trust. As a result, many women have reached out to DRF about their experiences with online discrimination and bullying, and these cases have provided the catalyst for us to streamline our activities and institutionalize the capabilities to accommodate in-person bullying. . By offering a sexual identity and confidential environment for those experiencing online abuse, the Helpline aims to solve systemic problems and limitations that women face. To ensure that a secure environment is built for its callers, the Helpline Support Staff has established robust policies regarding privacy, caller anonymity, and quality assurance. In a patriarchal culture such as ours, societal expectations and the concept of honour pose a significant barrier to combating cases of online abuse. As a result, the perpetrator survives several encounters, and online abuse remains a largely unreported crime. There have been several occasions where harassers have been arrested and convicted as a result of the passage of this law. After the victim submitted evidence of his involvement in online abuse, a professor from the University of Karachi was apprehended. Similarly, a few female faculty members at NCA Rawalpindi raised allegations of online abuse against the campus's director. After that, he was asked to resign.

After that, in the midst of the online abuse debate, female rights activists in Pakistan argue that victims should seek justice through a judicial process based on substantial and meaningful facts rather than condemning men in general and requesting assistance from social media users. According to them, the rise of anonymous allegations threatens to delegitimize the long-running fight against online abuse. Sharmeen Obaid C is one example who took help from twitter.

PECA ensures that internet users are secure. The responsibility, nevertheless, falls on the government and other relevant agencies to

educate the public about the law. More significantly, it is the responsibility of the educated class to raise consciousness about the law's practicality and legality. The government must develop a strategy to educate students in schools, colleges, and universities about Internet protection and freedom of speech. They must be taught how they can legally take up their cases. Article 18 of PECA states:

*" Whoever knowingly and publicly exhibits, shows, or transmits false information through any information system, and intimidates or damages the integrity or privacy of a natural individual, shall be punished with imprisonment for a period up to three years or a fine up to one million rupees, or both."*

After a report is filed, the matter is taken up by the FIA, which tracks down the perpetrator while respecting the complainant's privacy. If fully implemented, this legislation can help to alleviate online gender inequality and challenges to feminism. Furthermore, opinion leaders and media behemoths should emphasise the importance of educating the public about Internet safety precautions. While speaking out against abuse online is essential, legal procedures must be followed. There are currently regulations in place to deal with these issues. If these legal processes are not followed, then slamming harassers on social media sites like Twitter and Facebook amounts to nothing more than accusations and stoking controversies. PECA is a successful legal mechanism for preventing online abuse of women. [17]

## School Action

It's worth noting that many schools are implementing strategies to combat Cyberbullying, which is extremely significant. Since cyber-bullying is primarily a result of the internet's presence, many schools have limited the number of websites available to students in order to protect them from visiting places that could lead to them being a target of a cyber-bully. In addition, several governments have implemented anti-bullying laws and regulations that include cyber-bullying. They constantly watch teenagers' internet browsing at school and have purchased monitoring software to screen out problematic online habits and bullying, but they do not rely exclusively on it. Many educators work to inform students, teachers, and other members of the staff about the risks of online harassment. [18]

## Responsible People

Despite efforts to change laws and regulations and to put them into effect, what is concerning is that no legislation can truly prevent cyber-bullying. Since contact through the internet or mobile phones offers anonymity, many fake accounts are generated in order to tease or threaten people on social media platforms such as "Facebook" and "Myspace. there is no one who can take responsibility for this mess. there should be a way to tell when a fake account has vanished. Our culture encourages abuse, which makes it harder to solve the issue. The majority of violent crimes are depicted in video games, television, and other forms of mass media. As a result, children and teenagers become used to the notion of violence and accept it as the norm. The concept of cyber-bullying is unfamiliar to most parents. It's not entirely their fault; technology advances at a breakneck pace, and many of them are unable to keep up. Teenagers seldom discuss their issues with their parents, making it difficult for parents to assist their offspring. Many schools make the mistake of not adequately educating students or teaching them how to defend themselves. Children should have an understanding of online harassment in order to avoid any "injuries." It

is believed that only society as a whole can be held accountable for this problem. [19]

## Conclusion

To summaries, while the internet and cell phone communication systems make our lives simpler and play an important role in our actions, it is sad that they have been tainted and ruined by their misuse. The advantages of the internet and cell phones cannot be debated or enumerated; however, I am fairly confident that the disadvantages are numerous. “Online bullying is the intolerable face of digital media, and we need collective action through society to fix it,” according to Kevin Brennan. Schools must play a significant role, and this new guidance will assist them in more efficiently identifying and responding to cases of cyberbullying, as well as offering practical advice and information about how to avoid it. ″ [20]

Cyber-bullying is on the rise, and it affects almost everyone who owns and uses a computer or a cellphone, but the possibility of stopping or preventing it seems to be a long way off. Cyberbullying occurs in classrooms, out of schools, and anywhere, and since guardians do not have absolute ownership over their children's behaviour in and out of school, it is difficult to track bullies' plans. Although overall school violence is decreasing, bullying behaviours have increased by 5%. Furthermore, there were several suicide deaths as a result of cyber-bullying in the last months of 2010. There are several reasons why anyone would bully someone else, and there are even more traps that might lead the harassed person to remain silent and add to the massive issue. After doing a lot of research, I'm not sure if this whole scenario can be avoided, but hoping it can at least be reduced. It seems that there is no way to avoid it because most states in the United States lack laws that specifically addresses cyber-bullying. Because of the anonymity of cyberbullying, even where regulation exists, it lacks the ability to significantly minimise it. This might even be a great research question for another extended essay. “Should the internet offer anonymity and the option to keep one's identity hidden ” Existing legislation in the states mentioned that United States has only worked in a few cases where the bully has not concealed his identity. Parents especially must not forget that thy have to protect their children. Because bullying via the internet and mobile phones cannot be completely eradicated, the next best option is to make children immune to it. It is important to teach children how to stop it and move on with their lives. They should be taught how to avoid being used as victims by bullies. Parents should assist their children in developing a strong personality. [21].

## References

1. Rehtaeh Parsons , Nova Scotia and 15-year-old Amanda Todd case

2. Leanne Lester et al., "Problem behaviours, traditional bullying and cyberbullying among adolescents: longitudinal analyses" (2012) 17: 3-4 Emotional and Behavioural Difficulties 435 at 436.

3. Ibid. at 443. https://www.justice.gc.-ca/eng/rp-pr/other-autre/cndii-cdnci-i/p1.html

4. Michael A. Couvillon and Vessela Ilieva, "Recommended Practices: Cyberbullying" (2011) 55:2 Preventing School Failure 96 at 96-97.

5. Justin W. Patchin and Sameer Hinduja,

"Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying" (2006) 4:2 Youth Violence and Juvenille Justice 148 at 150.

6. Canada, Standing Senate Commiteee on Human Rights, Cyberbullying Hurts: Respect for Rights in the Digital Age, (Ottawa) online: http://www.parl.gc.ca/Content/SEN/Committee/411/ridr/rep/rep09dec12-e.pdf (last accessed: May 24, 2013).

7. See: http://www.cyberbullying.ca/. See also Media Smarts' website on "How Kids Cyberbully", online: http://mediasmarts.ca/cyberbullying/how-kids-cyberbully.

8. L'Enquête québécoise sur la santé des jeunes du secondaire 2010-2011 : Tome 2 - Le visage des jeunes d'aujourd'hui: leur santé mentale et leur adaptation sociale, Institute de la statistique du Quèbec, p. 30, online: www.stat.gouv.qc.ca (last accessed May 24, 2013).

9. Samuel Perreault, "Self-reported Internet victimization in Canada, 2009" (September 15, 2011) Juristat, Canadian Centre for Justice Statistics, catalogue no. 85-002-x, online: http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-eng.pdf.

10. Nandoli von Marées and Franz Petermann, "Cyberbullying: An increasing challenge for schools" (2012) 33:5 School Psychology International 467 at 469.

11. Ipsos Reid, online survey of 422 Canadian teenagers one-in-five (20%) teens indicated they have witnessed someone they know being bullied on social networking sites and nearly one-in-ten (8%) stated that they themselves have been victims of online bullying on social networking sites. One-in-seven (14%) of the teenagers surveyed indicated that they had been victims of mean or inappropriate comments on social networking sites.

12. William V. Pelfrey, Jr. and Nicole L. Weber, "Keyboard Gangsters: Analysis of Incidence and Correlates of Cyberbullying in a Large Urban Student Population" (2013) 34:1 Deviant Behavior 68 at 72, Faye Mishna et al., "Risk factors for involvement in cyberbullying: Victims, bullies and bully-victims" (2012) 34 Children and Youth Services Review 63 at 63.

13. William V. Pelfrey, Jr. and Nicole L. Weber, "Keyboard Gangsters: Analysis of Incidence and Correlates of Cyberbullying in a Large Urban Student Population" (2013) 34:1 Deviant Behavior 68 at 71-72.

14. Research indicates that 98% of Canadian youth access the Internet and communication technologies on a daily basis. Faye Mishna et al., "Risk factors for involvement in cyberbullying: Victims, bullies and bully-victims" (2012) 34 Children and Youth Services Review 63 at 63.

15. Ahmed Umer Shoaib May 15,2018 https://nation.com.pk/15-May-2018/curbing-online-harassment-through-law

16. The Introduction To Cyber Bullying

Media Essay. Retrieved from https://www.ukessays.com/essays/media/the-introduction-to-cyber-bullying-media-essay.php?vref=1

17. https://nation.com.pk/15-May-2018/curbing-online-harassment-through-law

18. Patricia W. Agatston, Robin Kowalski, Susan Limber, Students' Perspectives on Cyber Bullying, Journal of Adolescent Health,Volume 41, Issue 6, Supplement,2007, Pages S59-S60, ISSN 1054-139X, https://doi.org/10.1016/j.jadohealth.2007.09.003.

19. Muhammad Imran Rasheed, Muhammad Jawad Malik, Abdul Hameed Pitafi, Jawad Iqbal, Muhammad Khalid Anser, Mazhar Abbas,Usage of social media, student engagement, and creativity: The role of knowledge sharing behavior and cyberbullying, Computers & Education, Volume 159, 2020, 104002, ISSN 0360-1315, https://doi.org/10.1016/j.compedu.2020.104002.

20. Amy L. Hequembourg, Jennifer A. Livingston, Weijun Wang, Prospective associations among relationship abuse, sexual harassment and bullying in a community sample of sexual minority and exclusively heterosexual youth, Journal of Adolescence, Volume 83, 2020, Pages 52-61, ISSN 0140-1971, https://doi.org/10.1016/j.adolescence.2020.06.010.

Sundus *et al.LGU (IJECI)* 2020

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 4 issue 4 Year 2020

# Overview of Security Measures in Big Data

**Sundus Munir[1] Afrozah Nadeem[2], Syeda Binish Zahra[3], Sadia kousar[4]**
sundusm1@gmail.com afrozah@gmail.com,,
binishzahra@gmail.com[3], sadiakousar@gmail.com[4]

University of Engineering and Technology[2]
Lahore College for Women University[1,4]
National College of Business Administration & Economics (NCBAE)[3]

## Abstract:

Big data refers to the huge volume of data that is being produced by different organizations after every second. It is hard to handle such volume of data, therefore this data is combined and managed through the servers of organizations using complex algorithms. Data is currently most important assets of any organization in every field with which many operations can be performed. Big Data exerts different properties those are volume, velocity, veracity and variety. Now there are different threats regarding the security of big data. Organizations are using different methods to secure big data. Big data security measures include architecture security, infrastructure security and data privacy. In this paper multiple security concerns are discussed and how they can help organizations to secure their data.

**Keyword:** Big Data, Cloud Computing, Hadoop, Encryption.

## 1. Introduction

Big Data is the term that describes the large volume of the data that is collected through different sources. Big data help the organizations to grow in different sectors. Big data is very complex as compared to traditional software's that is linked to data processing. Big data processing requires the system with more statistical power. Big data is not only about collection of data but also there are different challenges like how to capture the data, its storage, analysis, transfer and updation.

Big Data analytics tools and techniques are rising in demand due to the use of Big Data in businesses. Organizations can find new opportunities and gain new insights to run their business efficiently. These tools help in providing meaningful information for making better business decisions.

The companies can improve their strategies by keeping in mind the customer focus. Big data analytics efficiently helps operations to become more effective. This helps in improving the profits of the company. Financial data scientists use big data to predict

which stocks will succeed and when future crashes are likely to occur. Banks also see big data as a way to increase their revenue.

Big data grows rapidly because numerous of devices are interacting with system. Every interaction generates series of data bytes which includes transaction, reports, logs and documents. Since 1980 the world's technological per-capita [1] capacity to store data has doubled every forty months and IBM added a update that since 2012 the data generation is increased 2.5 extra bytes.

Big data contains sensitive data of organizations and individuals. For example, companies that provides cellular services collects data of numerous Calls, SMS and internet data which is directly linked to the privacy of the consumers. Company use this data to store, analyse, update, search, transfer through complex machines. This arises a alarming thought that if some third party breach into big data and collects sensitive information it might cause a big problem to the privacy of customers. Big data security is very crucial that the US National government financed $200 million to Big data research [2]. This portray that big data is expanding vastly and exerting its impact on daily life.

Big data is making a huge difference in many fields like healthcare [27]. Insurers and providers are working on combining data from different sources such as claims, X-rays, doctor's notes, and prescriptions. Many believe that if healthcare data better integrated it could provide better care at a lower cost.

## 2. What is Big Data?

Big data is used when there is enormous volume of data regardless it is structured or unstructured. The traditional systems and databases cannot handle this enormous volume of data. It requires a massively parallel software running on hundreds of server systems. Big data can be characterized and understood with the help of 4V's which not only exhibit the complexity of big data but also its speed [3]. The 4V's are

Volume
Variety
Velocity
Veracity

### 2.1 Volume:

The term volume in big data is used to show the amount of data that is generated by some company or organization. The quantity of data not only refers to the value of data but also potential of the information derived from the data. The collection of massive data in structured and unstructured form required connection of servers with the dynamic storage capabilities. Several Companies like Amazon [4] is providing storage services which may vary from user or company requirement.

### 2.2 Variety:

In big data different software's and systems are connected and they generate different data in various formats. For instance, a media company generate several copies of audio, video files while a software house generate data of different formats like logs, sheets, software versions and some unstructured data which is not being explored using traditional software's. This shows that how much variety of data is processed in big data.

### 2.3 Velocity:

To understand what velocity is in big data there are two situations. One is the speed of generation of data with in a system and second is speed of data storage. Like a telephone

company generate hundreds of thousands of data like logs and files in seconds. Hence, it is about to meet the demands of speed. The term velocity also refers to the speed of the data processing that is stored in the systems.

### 2.4 Veracity:

The term veracity refers to the trustworthiness of big data. The uncertainties that are found in data because of incompleteness, deception and ambiguities reduce the quality of data. The quality of data that is stored depends on the analysis of data which is directly linked to the Veracity of data.

## 3. Big Data Analysis

In big data analytics mostly the process of data mining and analysing occurs. This process can help to achieve business knowledge and operational skills to unprecedented scale. Big data analysis helps to identify the trends in the data collected by business. Big data analysis helps in examining chunks of data which results in finding the un-known correlations, improved customer services, better business strategies, marketing patterns and efficient customer support. It includes different processes that are predictive analysis, text analysis. Here are some of the advancements that are occurred due to the field of big data.

- Cloud Computing [5] and data centres acquired flexible storage and computing resources to manage and apply operations on data collected from the business.

- Different frameworks are designed to manage and store large quantity of data. Best example of the framework is Hadoop which helped multiple users to get advantage of cloud computing [6].

- Storage cost has been reduced since last few years that a user can acquire hundreds of giga bytes from computing and data storage purposes in few bucks.

- Big data is very helpful in machine learning. By following the results and patterns of big data new algorithms for machine learning has been designed.

- Big data has created many job opportunities like Big Data Analyst, Big Data Engineer, Business Intelligence Consultants, Solution Architect, etc [7].

## 4. Stages of Big Data

Here are few stages of big data that are followed in the process of making the data useful for any particular goal. After following these stages organization can gather valuable piece of information from data.

### 4.1 Understanding of Business:

Goals are necessary to understand that what is best for achieving business point of view. In the business how data can be beneficial and what measures and parameters should be defined before processing the data. The problem statement is target and then Decision Model is utilized for the goal achieving.

### 4.2 Understanding of Data:

For this purpose, data is collected for understanding so that information derived from data is accumulated. Data understanding also refers to the mining of data. After data is organized it can be used in achieving the goals.

### 4.3 Preparation of Data:

Data is prepared in the forms of tables and databases so that the quality data is acquired in the fastest way. Data is manipulated in the structured form like table to make it suitable

for next processes.

### 4.4 Data Modelling:

After all these steps a data mining model is selected. In data modelling it is easier to understand that how data flows to complete the system with the help of symbols and diagrams. Model is consisted of a scheme that fulfils the requirements of parameters in the systems.

### 4.5 Data Evaluation:

In data evaluation every chunk of data is reviewed with the deep analysis and logical reasoning. A model is selected for data processing and after that a survey is organized to make it clear that the model will successfully accomplishes the goals of the business.

### 4.6 Deployment:

Last step is the deployment of the model to finish the venture. During deployment of data Hadoop Tool is used to handle the changes of big data. In deployment data is being processed and analysed for the results [8].

## 5. Data Visualization in Big Data

In modern industry IOT (Internet of Things) refers to adopt new policies and methods. This not only result in generation of variety of skills and also reducing global competition stress regarding data handling. The total volume of data after internet of things has come increased to Thousand times more than the last decade. This revolution after inclusion of data in the industries and digital ecosystem is called Fourth Industrial Revolution (add reference). More devices that are connecting to the system are tools, plants, machines, auto mobiles, robots and they are producing data at very high rate. This data is being utilized by the big companies enabling to unlock the untapped possibilities in every field of life. The idea to produce fault free machines can be pursued in the light of big data because it will help to acquire the best performance levels. Data Visualization is big challenge in big data. There are different approaches that are being used for the data visualization and also multiple tools that are as follows [9]

- Plotly
- DataHero
- Tableau
- ZingChart
- Chart.js
- Google Analytics
- Dgraphs

These tools are being used for data visualization. For real time understanding and reasoning of big data, we work with supply chains to produce results i.e., manufacturing intelligence. [10]

## 6. Big Data Security

Within the new era of technological revolution there are also some issues that arise and some are becoming strong challenge for the technology. The same happened with the revolution of internet of things and big data. These issues are deeply linked to the volume and privacy of data. Traditional security measures, tools and management are not proper solution of these problems. Without building proper solutions of the problems arising in big data it will not achieve the required level of trust. According to group of people working on Big data in Cloud Security [11] Alliance stated that there are majorly four different aspects of Big data security that are as follows

- Infrastructure Security
- Data Management
- Data Privacy

- Integrity and Reactive Security

In the International Organization of Standardization these four topics have been used in the area of Big Data Security [12].

### 6.1 Infrastructure Security

There are technologies and frameworks that are being used in the infrastructure of big data to secure it. The discussion of these frameworks and technologies are must for big data security and especially for those which are purely based on Hadoop Technology. Most of the big data systems are based on Hadoop. Further following are some important points which discussing the infrastructure security [13].

- Security for Hadoop
- Architecture Security

#### 6.1.1 Security for Hadoop:

When we deal with the infrastructure security Hadoop is necessary. Hadoop platform uses map reduce programming model to process the data.[14] Researchers have proposed some models for the security of Hadoop in which includes the use

of new schema and creation of encryption keys and schemes. Hadoop ecosystem has a framework that is known with the name of Knox whose solemnly function is to manage security implementations across the Hadoop cluster. In Hadoop File Distributed system (HDFS) the encryption process works in such a way that there are zones defined and each zone is created by different directories. [15] Each zone is encrypted by some key. That unique key is called as DEK (data encryption Key) only client can decrypt the protected data and can use it. Hadoop has its unique feature of storing all keys in a server. So, this encryption key feature helps Hadoop to authenticate clients and data [16]. There is a scheme for data confidentiality that is called as Trusted Scheme for Hadoop Cluster (TSHC). This TSHC creates an architecture for Hadoop system which is improve the infrastructural security for big data [17].

#### 6.1.2 Architecture Security:

Rather than depending on a single architecture the security of the environment. HDFS with the combination of network coding and multi node reading there is less chances of vulnerability. Here is also a suggestion that the data centres should be built near to the data so that the data communication would face less risk. Sensitive fields should be encrypted with the algorithms and keys so that risk of manipulation and exposure of data to unknown entity is reduced. When data is encrypted, important point is key management. Such a mechanism should be implemented that keys will be generated on base of need.[18]

### 6.2 Data Management

Once all the data that system generates is collected in servers of big data. Here a new point arise how it should be managed. In order words what we need to do with data and if it is viewed in the sense of security how to securely manage it. These are some important points which fall under data managements. What are the security measures around the servers where data is collected? [19]. What are the security parameters when all this data is being stored in the servers? The main point is to protect the user's privacy and for that some parameters and levels should be set.

A very serious problem around big data that is how this data can be used. Different companies make different policies regarding data use. They can make it open for their clients if they agree to use this data purposely with restrictions. Recently an incident occurred

"Facebook–Cambridge Analytica Data Scandal" [20] in which data of public profiles and their interests have been used without their consent. That data has been used indirectly to manipulate the election results. This clearly shows that how data is valuable and if it falls in wrong hands then it can be fatal for not only an organization but also threat to entire nation. After this incident several governments apply new rules and govern some strict laws to protect the data because it is their privacy which is at stake mostly. Organizations have been working to create some new rules that will reduce this risk of mismanagement of data.

The key thing in the data management is sharing and without sharing there is no purpose of the entire system. Large amount of data is collected and shared on the servers and sometimes different companies with big data collaborates to launch a new service or product to handle risk and threats. so the risks and threats to data should be ended.

### 6.3 Data Privacy

Data Privacy refers to which and how data (stored in system) is shared with the third parties. Privacy is the most important measure linked to the people could be at stake [21]. This matter is also important to the organizations and companies who deal with big data and using it for their advantage. There is a thought emerging in researchers that there must be rules and laws to limit the use of the data. Companies should be allowed to use the data for their benefits but also secure the privacy of collected data. The privacy requirements should be specified for collecting, storing and processing the big data.[22]

There are different ways to secure the data and more ways are being introduced. One of them is cryptography and it is the frequently used method. The most famous cryptographic algorithms are Advanced Encryption Standard (AES) and RSA Algorithm. Along with these algorithms some other methods which would be implemented like firewalls, transport layer security and they act as virtual barrier in the access of data. The software's which are developed for the purpose of surveillance and tracking are very complex to implement on very large data. Along with the risk of exploitation of these software's, they require a staff with good technical skills and huge implementation cost. The very next and important point is access control for the data privacy in which the users who doesn't have a role towards the data should be blocked or restricted. Some authors refer to some frameworks in order to manage the access control features and some gave importance to the map reduce process.[23] The approach to data has to be confidential and for that purpose new techniques are proposed. CMD (Computing on Masked data) this scheme allows computations to be performed on masked data which will not only improves the integrity but also data confidentiality.

There are different ways to secure the privacy of data by making it anonymous. Such kind of mechanism should be used that either hide the data or remove the sensitive information automatically. There are two schemes which are used to make the data anonymous. First one is Top -Down Specialisation, it is natural and efficient for handling both categorical and continuous attributes. This top-down specialization data usually removes redundant structures for classification to make the data anonymous [24]. Second one is Bottom-up generalisation, this approach incorporates partially the requirement of a targeted data mining task into the process of masking data so that essential structure is preserved in the masked data. Once the data is masked,

standard data mining techniques can be applied without modification [25].

People are also using social media network and its popularity is increasing day by day. Different platforms of social media are introduced with different features. Organizations who run social media are well aware that how much data is collected and processed in their servers. Privacy is the most important aspect in the social media networks. [26]

### 6.4 Integrity and Reactive Security

One of the bases on which Big Data is upheld is the ability to get streams of information from various sources like in distinct format from different origins: either structural or un-structural data. This builds the significance of checking that the data's integrity is upright so it may be utilized appropriately. It can also be used to monitor security so as to detect whether system is attacked or not.

Integrity is very important it defines the trustworthiness, accuracy and consistency of data. During its life cycle it protects data from unauthorised modifications. It is one of the most important concepts in dimension of security. In Big Data environment, achieving integrity is very critical when attempting to manage different problems.

## Conclusion

This paper concludes the importance of big data. How data is being organized, collected, processed and what are the security threats. The next era of technology is mostly based on how organizations, Government and private institutes are using data for different goals and purposes. Therefore, multiple security mechanisms are suggested for companies. Each organization has set different steps and criteria to process the data into useful information. Security of big data involves the security of infrastructure, data management and privacy of data. In infrastructure security the Hadoop tool security is key point because it processes and communicate with the clusters of data. Architecture security is also important in every aspect in which we see what schemes are used, what are the locations, where physical systems are located and where data is being processed. Best way to secure data is to build data centres where data is being collected. Data Privacy is very important in big data security as previously explained the scandal of Facebook it shows how data can be used for manipulation of ideas and thoughts of people. Millions of people are somehow connected to systems and they are sharing information which is processed in some online systems. Data management is also important point in big data because if data is not managed properly with proper parameters, then it would give the results which are not required to achieve the goal for an organization. Organizations need to focus on the big data security if they really want to grow the company and build trust in the market.

## References

[1] IBM What is big data? – Bringing big data to the enterprise. www.ibm.com. Retrieved 26 August 2013

[2] K.Valli Madhavi, Dr.Y.Venkateswarlu ,Varsha Sharma ,Big Data Analytics for Security, 2018

[3] P. Kamaksh, Survey on Big Data and Related Privacy Issues, Voulme 03,Issue 12, pp.68-70,Dec 2014

[4] Cloud Storage Services–Amazon Web Services (AWS) – aws.ama-

zon.com/products/storage. Retrieved August 2014.

[5] Big Data Security – The Big Challenge Minit Arora, Dr Himanshu Bahuguna, 2016.

[6] Devaraj Das, Owen O'Malley, Sanjay Radia and Kan Zhang ―Adding Security to Apache Hadoop.

[7] Why is Big Data Analytics So Important? www.whizlabs.com/blog/big-data-analytics-importance - Retrieved 19 March 2018 .

[8] SURVEY OF BIG DATA SECURITY Snehalata Funde, Computer Engineering, BSCOER, Narhe, India.

[9] Big Data Visualization Tools Everyone in the Industry Should Be Using - Promptcloud.com, Reterived 24 Feburary 2016.

[10] A, Katal, Wazid M, and Goudar R.H. "Big data: Issues, challenges, tools and Good practices."., pp. 404 – 409, 8-10 Aug. 2013.

[11] W. Hao, "Secure Sensitive Data Sharing on a Big Data Platform", Tsinghua Science and Technology, vol. 17, no. 1, (2015), pp. 72-80.

[12] Wang, H.; Jiang, X.; Kambourakis, G. Special issue on Security, Privacy and Trust in network-based Big Data.Inf. Sci. Int. J. 2015

[13] A Novel Framework for Big Data Security Infrastructure, Manpreet Kaur, Saravajanik College of Engineering and Technology.

[14] Cugoala, G. & Margara, A. (2012). Processing Flows of Information: From Data Stream to Complex Event Processing. ACM Computing Surveys 44, no. 3:15.

[15] Priya P. Sharma, Chandrakant P. Navdeti, (2014), " Securing Big Data Hadoop: A review of Security Issues, Threats and Solution", IJCSIT, 5(2), pp2126-2131.

[16] Cohen, J.C.; Acharya, S. Towards a trusted HDFS storage platform: Mitigating threats to Hadoop infrastructures.

[17] Quan, Z.; Xiao, D.;Wu, D.; Tang, C.; Rong, C. TSHC: Trusted Scheme for Hadoop Cluster. In Proceedings of International Conference on Emerging Intelligent Data &Web Technologies (EIDWT), Xi'an, China, 9–11 September 2013.

[18] Frank, J.B.; Feltus, A. The Widening Gulf between Genomics Data Generation and Consumption: A Practical Guide to Big Data Transfer Technology. Bioinf. Biol. Insights 2015, 9 (Suppl. 1), 9–19.

[19] Wang, Y.; Wei, J.; Srivatsa, M.; Duan, Y.; Du, W. IntegrityMR: Integrity assurance framework for big data analytics and management applications. In Proceedings of the 2013 IEEE International Conference on Big Data, Silicon Valley, CA, pp. 33–40.

[20] 50 million Facebook profiles harvested for Cambridge Analytica in major data breach – www.theguardian.com, Retrieved 18 March 2018.

[21] What is Data Management? – NGDATA https://www.ngdata.com/what-is-data-management/ Reterived 31 March 2016.

[22] Xu, L.; Jiang, C.; Chen, Y.; Ren, Y.; Liu, K.J.R. Privacy or Utility in Data Collection? A Contract Theoretic Approach. IEEE J. Sel. Top. Signal Proc. 2015, 9, 1256–1269.

[23] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[24] Top-Down Specialization for Information and Privacy Preservation, Benjamin C. M. Fung, Ke Wang, Philip S. Yu.

[25] Bottom-up generalization: a data mining solution to privacy protection, Ke Wang ; P.S. Yu ; S. Chakraborty.

[26] Sundus Munir "Social Media and its Impact on Privacy", International Journal of crime Electronic Investigation (IJECI), (2018).

[27] Afrozah Nadeem, Sundus Munir, Syeda Binish Zahra, Sadia Kousar, "Challenges and Opportunities of Big data in health care" , International Journal of crime Electronic Investigation (IJECI), http://ijeci.lgu.edu.pk/index.php/i-jeci/issue/view/11/11

Binish *et al.LGU (IJECI)* 2020

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 4 issue 4 Year 2020

# LALR Parser Implementation using Grammar Rules

**Syeda Binish Zahra**
binishzahra@gmail.com
National College of Business
Administration & Economics (NCBAE

## Abstract:

Syntactic parsing deals with syntactic structure of a sentence. It refers to the grammatical arrangement of words in a complete sentence. A syntactic analysis of English words will be presented using bottom up parsing in which LALR parser defines the best syntax analysis. A compiler is constructed that generates token of the identifiers that are characters, alphabets, etc. using symbol table, checks for the syntax of sentence by dividing into phrases, generating errors, debugging them and giving us the correct sentence.

## Keyword:

## 1. Introduction

Compiler as we know is a program that takes one language as an input and translates into another equipment language which we plea. Compilers are broadly applicable and are used frequently in many unexpected areas. A compiler is said to be good that contain self-contained units that are ready to be executed [1]. Analysis and synthesis are two parts of compiler that further divides the operation of compiler in six phases.

Grammar is a set of language rules to create phases and sentences that convey meaning and those rules which involve meaning of words are called semantics and those that don't involve meaning are called syntactic. So both the terminologies mean a lot. Context free grammar (CFG) are the set of rules or productions that shows which element occur in a phase and in what order.

Many researches have been published on parsing methods for natural language. Here we want to parse the grammar of English language [2, 3]. Simply, there is a need of compiler that translates the syntax of English language. Syntax analysis is a fundamental area of research and is used in key areas of computational etymology for example in machine translation, information retrieval etc. this determination of syntax analysis is done by the help of parsing.

The main purpose of Syntax analyzer is to identify the syntactic structure of a sentence

and parsing them accordingly. A widely used mathematical system for exhibiting essential structure in natural language is context-free grammar (CFG) also known as phrase structure grammar. Parse trees are used to show the structure of the sentence, but they often contain dismissed information due to understood definitions [1]. Context-free grammar (CFG) was first defined for natural language by Chomsky in 1957 that consist of terminals, non-terminals and a production rule from non-terminal to terminal or another non-terminal.

## Methodology:

Many online and offline service/software are provided to frequently check the errors in our grammar for both syntax and semantic error. Researches are proposed and published on the parsing of natural languages. In the previous research, Parse trees are used to show the structure of sentence [4]. Firstly it shows the type of sentence, then the components of the sentence are identified. Again the grammar rules are checked, if the sentence parse through the defined grammar then the sentence is considered as syntactically correct. Otherwise it is syntactically incorrect. The context free grammar of the symbol will be defined along with the symbol table. The parts of speech tagger will also be the part of the compiler.

In many researches, the LL1 parser are used as top down parsing that starts checking from the start point mainly ROOT and comes downward towards the LEAVES (Ending point). Here the advantage of use of this is that it never waste time on subtrees and can go further deep to find the valid string. Rule based approach algorithms and part of speech tagger are used as the part of software. But the issue is that it waste time on trees that don't match the input. It compares the first word of the input with the leftmost branch of the tree. The need of writing this paper is the use of bottom up parsing such as LALR. As in some previous research papers, top down parsing are used.

Here in this research we will use bottom up parser that starts from the words in the input sentence and attempts to construct a parse tree in an upward direction towards the root. At each step or level the parser with look for the rules and the defined productions. The idea is to use LALR parser because of its effectiveness [5]. LALR stands for look ahead left right is a technique for deciding when reductions have to be made in shift/reduce parsing. Often, it can make the decisions without using a look ahead. Sometimes, a look ahead of 1 is required [6, 7].

Most parser generators construct LALR parsers. In LALR parsing, a deterministic finite automaton is used for determining when reductions have to be made. The deterministic finite automaton is usually called prefix automaton [8]. This look ahead parser uses look ahead sets. If a state has more than one reduction, or a reduction and a shift, the parser looks at the look ahead symbol, in order to decide what to do next. With LALR (look ahead LR) parsing, we attempt to reduce the number of states in an LR (1) by merging similar states. This reduce the number of states to the same as SLR (1) but still holds some powers of the LR (1) look ahead.

LALR parser starts with the idea of building an LR parsing table. These generated tables are less powerful than LR but more than SLR Techniques.

## Evaluation:

Bottom up parsing mainly focuses on shift reduce parser in which the stack hold grammar symbol and an input buffer holds the best of string to be parsed. But there are some limitation in shift reduce parser. Sometimes in this parser we need to look ahead. So, knowing the benefit of LALR parser we can easily check the grammar of our language. The context free grammar defines the production rules. Setting the production rules according to the program. The symbol table that adds new identifiers in memory, generate tokens according to their values. Here we are using English language so alphabets, special characters will be added as identifiers. Special and most frequently used words might also be stored for the semantic meaning of the sentence.

Using the LALR parser, the sentence can effortlessly be parsed with look ahead. Here the grammar in the CFG is Verb, pronoun, nouns, articles, adjectives, and other grammatical verses. The CFG just defines syntax but the structures are not specified. Firstly turning a string/file into a series of tokens during a phase referred to as "Lexical Analysis" [3]. Once we have a collection of tokens, we match them against a "grammar." Grammars are simple languages that are used to bootstrap more complex languages [2]. They consist of simple mapping rules that indicate what rule to evaluate next. Then the production rules are checked and proceeds accordingly.

The LALR parser has more language recognition power than the LR (0) parser, while requiring the same number of states as the LR (0) parser for a language that can be recognized by both parsers. This makes the LALR parser a memory-efficient alternative to the LR (1) parser for languages that are not LR (0).

## Conclusion and Future Work:

This paper focuses on the syntax analysis for natural language using LALR parser. This is an approach to check the correctness of the sentence. This approach cannot achieve the accuracy and checking up to 100 % but still works accurately. Here in future its performance can also be enhanced and this can further be enhanced by constructing a compiler that translates URDU words using this technique.

## References:

[2] Haider, H.; Rosengren, I. Scrambling; Sprache und Pragmatik: Lund, Sweden, 1998.

[3] Kübler, S.; McDonald, R.; Nivre, J. Dependency parsing. Synth. Lect. Hum.Lang. Technol. 2009, 1, 1–127.

[4] Kuhlmann, M. Mildly non-projective dependency grammar. Comput. Linguist. 2013, 39, 355–387.

[5] Skut, W.; Krenn, B.; Brants, T.; Uszkoreit, H. An annotation scheme for free word order languages. In Proceedings of the 5th Applied Natural Language Processing Conference, 31 March–3 April 1997; pp. 88–95.

[6] Ranta, A. Grammatical Framework: Programming with Multilingual Grammars; CSLI Publications: Stanford, CA, USA, 2011.

[7] Ljunglöf, P. Expressivity and Complexity of the Grammatical Framework. Ph.D. Thesis, Göteborg University, Gothenburg, Sweden, 2004.

[8] Kallmeyer, L.; Maier, W.; Parmentier, Y.; Dellert, J. TuLiPA-Parsing extensions of TAG with range concatenation grammars. Bull. Pol. Acad. Sci. 2010, 58, 377–391.

[9] Kallmeyer, L.; Parmentier, Y. On the relation between multicomponent tree adjoining grammars with tree tuples (TT-MCTAG) and range concatenation grammars (RCG). In Proceedings of the Second International Conference on Language and Automata Theory and Applications (LATA 2008), Tarragona, Spain, 13–19 March 2008; pp. 263–274.

# Editorial Policy and Guidelines for Authors

IJECI is an open access, peer reviewed quarterly Journal published by LGU Society of Computer Sciences. The Journal publishes original research articles and high quality review papers covering all aspects of Computer Science and Technology.

The following note set out some general editorial principles. A more detailed style document can be download at www.research.lgu.edu.pk is available. All queries regarding publications should be addressed to editor at email IJECI@lgu.edu.pk. The document must be in word format, other format like pdf or any other shall not be accepted.
The format of paper should be as follows:

- Title of the study (center aligned, font size 14)
- Full name of author(s) (center aligned, font size 10)
- Name of Department
- Name of Institution
- Corresponding author email address.
- Abstract
- Keywords
- Introduction
- Literature Review
- Theoretical Model/Framework and Methodology
- Data analysis/Implementation/Simulation
- Results/ Discussion and Conclusion
- References.

Heading and sub-heading should be differentiated by numbering sequences like, 1. HEADING (Bold, Capitals) 1.1 Subheading (Italic, bold) etc. The article must be typed in Times New Roman with 12 font size 1.5 space, and should have margin 1 inches on the left and right. Length of paper should not be longer than 15 pages, including figures, tables, exhibits and bibliography. Table must have standard caption at the top while figures below with. Figure and table should be in continues numbering. Citation must be in according to the IEEE 2006 style

# LAHORE GARRISON UNIVERSITY

Lahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in the Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

## VISION

Our vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

## MISSION

At present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

**Contact:** For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:
Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
Email: ijeci@lgu.edu.pk


**Published by: Digital Forensics Research and Service Center , Lahore Garrison University**