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

International Journal for Electronic Crime Investigation

(IJECI)

VOL: 5
ISSUE: 3 Year 2021

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 5(3) Year (2021)

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 5(3) Year (2021)

CONTENTS

LGU International Journal for Electronic Crime Investigation
Volume 5(3) Year (2021)

Attacks on the Critical Infrastructure of Pakistan

Kaukab Jamal Zuberi
Cheif Editor

It was May 29, 2009, when the White House released the text of President Obama's speech on establishing a new cybersecurity office in White House. He mentioned "This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.

So, cyberspace is real. And so are the risks that come with it."

In 2013, Snowden revealed that Pakistan, after Iran, was the most targeted country for surveillance by National Security Agency.

Microsoft also revealed that Pakistan witnessed the highest malware attack in mid of 2015. Later senate committee was shaped to bring a report on cyber threats and the committee revealed that Pakistan was among the top countries under foreign espionage. A country that is hostile to Pakistan is heavily attacking Pakistan. India has been hacking websites of the Pakistani government since 1998 with mostly denial-of-service (DoS). The reports show that between 1999 to 2008 nearly 1600 Pakistani websites were targeted by Indian hackers.

The websites of NAB, Education Ministry, NADRA, Ministry of Foreign Affairs, Finance Ministry and State Bank of Pakistan were hacked previously.

Prevention of Electronic Crime Act (PECA) came into force in 2016. Critical Infrastructure is defined under the act as follows:

"(x) "critical infrastructure" means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in,

(a) major detrimental impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or

(b) significant impact on national security, national defense, or the functioning of the state: Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub¬paragraphs (i) and (ii) above, as critical infrastructure as may be prescribed under this Act;"

Section 6,7,8 of PECA defines the offences against the critical infrastructure, while section 10 link these offences to Cyber Terrorism as follows:

"10. Cyber terrorism: - Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to,—

(a) coerce, intimidate, create a sense of fear, panic, or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or

(b) advance inter¬faith, sectarian or ethnic hatred; or

(c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both."

As per the definition of PECA, earlier cyber-attacks were the act of cyber terrorism and the attacks on the critical infrastructure after August 2016 were punishable as per the punishments defined under the Act.

In July 2021, Pakistan announced its long due National Cyber Security Policy. One of the guiding principles of the policy was that the government "Will regard a cyber-attack on Pakistan CI/ CII as an act of aggression against national sovereignty and will defend itself with appropriate response measures." The policy mentioned that every organization will be responsible for its cyber security and in case of a cyber-attack, the government will take lead the national response with help of the public and private sector.

However, this policy was announced without timelines and identifying the responsible organization to implement the national cybersecurity policy. The sense of urgency to safeguard our critical cyber infrastructure was missing from our National Cybersecurity policy.

August attacks on FBR infrastructure is a classic example of the poor handling of the incidents. The role of government agencies in determining those responsible for these attacks and ultimately punishing them is yet to be seen. In both the incidents, Microsoft Hyper V terminals were involved. Poor defense mechanism and sheer incompetence was revealed during this attack. The former Chief US diplomat for South Asian Affairs, Alice Wells, during her visit to Pakistan accused FBR of using a pirated version of Microsoft Hyper-V software and warned that FBR might become a target of cybercrime due to the use of a pirated software.

There are at least three versions of how hackers gained access to the critical infrastructure of FBR. The first version from technical wing of FBR stated that hackers gained accessed by using the vulnerabilities of Microsoft Hyper V terminals. The second version stated that the hackers disrupted the system by hacking the login ids and passwords of the data centre administrators and the third version, which was published in the report prepared by a local firm stated that the hackers used Spear-phishing emails as the medium for this breach. As a result of these lukewarm and complete the file type responses, HackRead, which is a news platform that centres on InfoSec, Cyber Crime, Privacy, Surveillance and hacking news reported that the confidential data of taxpayers was stolen in this breach. Furthermore, HackRead claimed that FBR's data was put on sale on a Russian Forum for $30,000.

This was an act of Cyber Terrorism, and the investigation lacked the vigor used to solve terrorism cases. The minister of technology announced on November 02, 2022, that millions of cyber attacks were being made in Pakistan every day.

Pakistan lacks a coordinated effort to combat the increasing threat on its critical infrastructure and critical information infrastructure. Immediate steps should be taken to develop a comprehensive strategy to mitigate these threats. As a way forward, it is suggested:

- To ensure the coordinated efforts across the government a national coordinating agency should be created develop a new comprehensive strategy to secure Pakistan's information and communications networks.
- All the key players – public and private - should be involved in this process of developing comprehensive cyber strategy.
- The government should collaborate with industry, by developing public private partnerships, to find technology solutions that ensure our security.
- Investments should be made in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. The government identify the organizations involved in cyber security research through out the country and support them.
- A national campaign to develop the awareness and digital literacy should be launched through out the country, from our boardrooms to our classrooms.

The News, a leading daily newspaper reported on June 30, 2021, "In a recent development, India is now ranked at No 10 at the Global Cyber Security Index, up from No 47 in 2019, as per a study by the United Nations. According to the study, the same index ranks Pakistan at No 79, foreign media reported."

We are living in the world of digital revolution and adopting a right strategy and swift implementation, will ensure our success in achieving the goal of creating Cyber Secure Pakistan.

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. 5 issue 3 Year 2021

Dominant Role of Forensic Evidence in Multidimensional Crimes Over Other Types of Evidence in Sexual Violence, Torture, Rape and Killing against 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] Dr Waqar Azeem PhD (Micro-Electronics Engineering); M.Phil; BS (Hons)
Assistant Professor, Department of Computer Science (LGU), Lahore
[3]Mujtaba Asad MS (Computer Science);MS (Electronics) BS(Hons); PhD Scholar,
School of Electronics Information & Electrical Engineering, Shanghai Jiao Tong University
Shanghai China

Abstract:

The trend in multidimensional crimes of Sexual Violence, Torture, Rape and Killing of Innocent Women and Children is exponentially increasing. The impact in the society is extremely adverse and unhealthy causing agony and mental torture to the common person. The life of citizens, women and children is not safe. The abduction of children under 16 accompanied with rape and torturous killing is becoming prominent and similarly women are victims. Their dead bodies are normally disposed of near city/village waste filth depot. On the other hand, children of religious schools mostly orphans are victims of "religious instructors", who are apparently out of the scope of law enforcing agencies. The "religious instructors" inflict and impose rigorous punishments including Sexual Violence, Torture, Rape and Killing. The character of "religious instructors" of the privately managed schools (madrassas) seems highly unreliable. The voice of their victims not heard in the nearby surroundings and neighborhood of society. Some rich and influential people with a blend of western culture, living without peace of mind are involved in heinous, monstrous, atrocious, odious, terrible multidimensional crimes of Sexual Violence, Torture, Rape and Killing of Innocent Women and Children. The authors of this paper have been advocating that the state, courts and law enforcement agencies must implement a strong deterrent strategy, preventive measures with restrictive approach to restrain such crimes. There must exist a real deterrent force in society to combat such crimes committed in series. The paper presents case studies to analyze and compare circumstantial evidence, the forensic evidence with that evidence tendered by eye- witnesses. Can the prosecution entirely rely upon the forensic evidence and circumstantial evidence in court of law? The paper addresses this question of law. The most sever part of the our assertion is who will control heinous offences of abduction, sexual violence, torture, rape and killing of innocent women and children, the legislation, the executive of the country, the courts or the law enforcement agencies?

Key words: Evidence, abduction, murder, Rape, mutilation of human body.

1. Introduction

In this paper, we present case studies to highlight and explain the essence of various kinds of forensic and digital evidence. The authors of this paper have been projecting the

core issues of the forensic evidence in various research papers [1] to [12]. The idea of strengthening the legal frame work and to strengthen prosecution has been discussed in [1], [2] and [3]; particularly in criminal cases related to evidence in terrible crimes of sexual violence, abduction, abuse, torture, rape and killing against innocent women and children. In [4], [5] [6] and [7], the present authors have advocated the following important assertions:

- Need to promulgate new strong legal framework for women and children for protection against offences of torturing, abusing or killing.
- Standardization of digital forensic evidence, its attaining, protection and presentation in court of Law using FBI techniques by FIA.
- Proposals to amend the Prevention of Electronic Crimes Act, 2016 (PECA) to facilitate Investigating Agencies, Courts and Prosecution, for proper use of Electronic Devices and effective implementation of relevant Law.

In [7] to [12], we the authors of this paper have discussed important applicable legal notions and main points:

- Electronic Devices must be used to Investigate Offences of Torturing, Abusing, Molesting Assaulting or Killing the Innocent Children,
- To make the task of prosecution effective using digital forensic evidence during investigation and court proceedings.
- Procuring confessional evidence of criminals, its significance as compared to forensic, digital and other oral evidence of witnesses and to prioritizing one over the other for effective case building,
- DNA fingerprints, facial prints and other digital forensics are most important as evidence in criminal investigation and court proceedings.

The terms morality and ethics are frequently used interchangeably, in literature in order to express exact vengeance, retaliation, and revenge on innocent people, including women and children, Some members of society are becoming enraged, irritated, vengeful, offensive, furious, and reactive. Furthermore, we are certain that the application and enforcement of Islamic law is required in accordance with the inherent principles of the law. Paralegals work behind the scenes, but their tireless work can be critical in helping lawyers crack their cases. There are a variety of different types of law you could dedicate your professional life to. The options for a fulfilling paralegal career are vast. As we work toward becoming a paralegal, it is beneficial to be familiar with the various types of evidence that may encounter throughout our career.

The main purpose of this paper is to highlight the preposition that in case of absence of sufficient eyewitnesses, how to present the case successfully based on available strong circumstantial evidence, the digital evidence and other type of forensic evidence collected from scene of crime. Depending upon the merits of the case and available evidence, one need to choose kinds of evidence to focus in order of merit. There are two main types of evidence i.e. the direct and circumstantial. The

direct evidence directly links a defendant to the crime, for example, eyewitness on oath; whereas the circumstantial evidence suggests that, a person committed a crime. Other kinds of evidence are narrated in Table 1.

Table 1: Categories of Evidence. Source: [13]

Admissible evidence	**Character evidence**	**Circumstantial evidence**	**Corroborating evidence**	**Demonstrative evidence**	**Digital evidence**
Direct evidence	**Documentary evidence**	**Exculpatory evidence**	**Expert witness evidence**	**Forensic evidence**	**Hearsay evidence**
Inadmissible evidence	**Individual physical evidence**	**Insufficient evidence**	**Physical evidence**	**Testimonial evidence**	**Trace evidence**

The real evidence is also termed as Physical evidence, which mentions the material body or any object collected from scene of offence and relevant to crime committed. For example, a gun, pistol, or other sharp edged knife or weapon, a shoe print, bullets lying on floor, or even tiny fibers from a piece of fabric, ropes or an item of clothing worn by the perpetrator**.** The physical evidence is concerned with and related specifically to the individual for example DNA or the fingerprints on the pistol from which bullet fired. Before the presentation of evidence, in the courts of law, we must examine the availed different types of evidence into two groups with respect to the impact such as admissible evidence and inadmissible evidence, then perused, and formally presented before the judge.

2. Forensic and Digital Evidence in Multidimensional Offences

The forensic evidence based on the science and plays pivotal role as reliable evidence, which may lead towards conviction of an offender. It is refereed and denoted to as scientific evidence/ Forensic evidence is often among the most helpful types of evidence in criminal litigation; that is based on knowledge that has been developed by using the scientific method. As such, the basis for admissible forensic evidence; it has been hypothesized, tested and accepted within the scientific community and courts. This includes **things like DNA matching, fingerprint identification, hair evidence, fiber evidence** and more. The trace evidence is prepared using two objects together, like **gunshot remainder, hair, fibers, soil, wood and pollen; helpful for linking the criminal (defendant)** and/or a victim to a mutual location. After obtaining the forensic evidence, the expert presents it to investigators as well as in the court. Expert witnesses are permitted to testify about matters within their field of expertise evidence from witnesses. The majority of what we see on TV in a typical courtroom drama is testimony. This is when a witness is called to stand to state under oath before a judge and jury. In a trial, witnesses can be beneficial by both, the prosecution and the defense. When prosecutors question prosecution witnesses, this is direct examination; when questioned by defense attorneys, referred to as cross- examination. A forensic analyst testifying about the results of a DNA test, a doctor testifying about an X-ray analysis, or a fingerprint analyst testifying about findings related to prints lifted from a crime scene or weapon are examples.

The digital evidence is most important to collect from electronic devices. Nowadays, in our technologically connected world, digital evidence has become critical, as computer data can leave a trail to a wide range of crimes. Any relevant information that is stored or transmitted in binary form is digital evidence. This includes anything found on a computer hard drive, a cell phone, a flash drive, and similar devices previously used only in the prosecution. No one can deny the importance of other types of evidence such as documentary evidence, demonstrative evidence (contained in documents) and the habit evidence. The character evidence establishes the previous conduct of the offender in the context of present offence.

3. Multidimensional Crimes Against Women and Children

We define the Multidimensional_crime in a case, committed by one, or group of persons involving a series of crimes against a person or group of persons, For example, a multidimensional crime may involve abduction, sexual violence, abuse, torture, rape and ultimately killing, all interconnected, integrated, interlinked and interwoven. In this section, the reliance and facilitation of research is mainly be based on the principles determined in [3]. The number of cases involving innocent women and children is steadily increasing. The perpetrators are engaging in sexual intimidation and harassment, as well as a high level of torture and murder as 'modus operendi'.The prosecution witnesses are the foundation of the criminal case in court. Because they know the relevant information and knowledge about the offence, the criminals and their aliases continue to pursue witnesses in order to prevent and avert evidence in court. Therefore, the reliance on digital and forensic evidence gains importance to strengthen the prosecution. According to [14], Zina Ordinance established by Pakistan's legislative criminal law, addresses fornication, adultery, and incest, as well as their evidentiary standards and penalties, treating them as similar crimes. If such evidentiary requirements are met. Quran specifies death by stoning or public flogging for all such offences as follows:

Let us quote from [15] 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).

The haddood laws are of special concern as for as this research paper is concerned. Under Islamic law, hudood 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. The Qur'an

mentions several hudood offences and, in some cases, prescribes penalties for them. For punishment however strong evidence is required. As for as homosexuality is concerned, According to [16], Islam is clear about its probation. Regarding the punishment for homosexuality, there is a consensus the Shafi, Maliki, and Hanbali schools generally prescribe the death penalty for penetrative same-sex intercourse. Consensus among the four leading Sunni schools of thought and most Islamic scholars that homosexual acts are a major sin and may be punishable by death. The Holy Quran has described three kinds of punishments that were meted out to the people of Lut (a.s.), one was a terrible scream and shriek, the second was the shower of stones that rained upon them, and the third was that the earth turned upside down. After mentioning the last calamity, it is said in Surah Hud:**"Marked (for punishment) with your Lord and it is not far off from the unjust."** (Surah Hud 11:83). Hazrat Imam Ali ar-Reza (a.s.) has said, "Refrain from adultery and sodomy, and this sodomy is worse than adultery. These two sins are the causes of seventy two ills of this life and the Hereafter." (Fiqh-e-Reza). The Quran has used the word 'indecency' for adultery in the way it has also used it for sodomy; Allah says in Surah Araf: "And (we sent) Lut when he said to his people: What! Do you commit an indecency which anyone in the world has not done before you?"

"Most surely you come to males in lust besides females. Nay you are a prodigal people". (Surah Araf 7:80-81). What could be more indecent than the act where man squanders away his sperms in a way prohibited by Allah instead of allowing them to reach the wombs of women to ensure the continuation of the human race? Sodomy and homosexuality are denounced in Surah Hud, Surah Ankaboot, Surah Qamar, Surah Najm in addition to Surah Araf; so that the people are fully warned. Allah has strictly forbidden such a loathsome act.

4. Permanently Achieving Deterrence Effect

In light of this, the National Research Council's study [17] deterrence and the Death Penalty investigates whether existing data provides a scientific basis for determining whether and how the death penalty affects murder rates. According to a new report by the Committee on Law and Justice, the available research on the effects of capital punishment on murder rates is insufficient to determine whether the deterrent effect has been effective. According to [3], the death penalty is enforced and exercised 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 publically. Rape in Saudi Arabia is 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. The death penalty is usual as prescribed under law in Bangladesh, China (see Table 2), India, Iran and in some cases in Pakistan. According to [3], Pakistan is a country in South Asia. The gang rape suspects in Pakistan be punished to death or life imprisonment under the (PPC) Pakistan Penal Code. In the United Arab Emirates, forced Rape with a woman is punishable by death. According to [17], statistics show that the death penalty, when applied publicly, has a significant deterrent effect on crime rates in China, particularly in countries such as Saudi Arabia.

Table 2: Offences qualified for death penalty. Source: [3]

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

5. Cases Involving Multidimensional Crimes

This section of the paper presents well-known criminal cases involving multidimensional crimes. We select first two cases from [3] for analysis. After a brief review, a comparison presented, regarding how case becomes stronger for the prosecution based on various types of evidence given in table 1.

5.1: Case study 1:

Zainab Ansari's Murder case contested without any eye-witness

Table 3: Facts of the case:

Sr#	Details	
1.	Name of 8 years girl murdered	Zainab Ansari
2.	Name of Accused	Imran Ali
3.	City	Kasur, Punjab
4.	Previous history	Involved in at least nine rape-cum-murder of minors confessed by him
5.	Modus operandi	Abduction by persuasion and killing by homicide via strangulation
6.	Offences committed:	Abduction, captive (kept girl in confinement for 5 days), torturing, rapping, and killing; threw dead body in garbage heap ; as well as for committing a terrorist attack
7.	Evidence	The accused's confessional declaration, testimonies, oral proof, forensic evidence, DNA report
8.	Prominent Feature of case	Prosecution based the case on strong circumstantial and forensic evidence
9.	Punishments:	21 counts of capital murder, three life terms, and a total of 23 years in prison. The court has also imposed a Rs 4,1 million fine. The death penalty was implement.

Only solid facts gathered by police and presented successfully in court by the prosecution allowed Zainab to justice. Riots erupted almost immediately in Kasur, as result of the heinous nature of the murder. The Supreme Court of Pakistan dismissed Ali's appeal against his death sentence for the rape and murder of Zainab due to solid facts, recalling that the appellant would have confessed to the crime.

5.2: Case Study 2:

Case regarding rape of a woman on highway

The goal of this case study is to demonstrate the critical importance of proper witness procurement and presentation in a court of law. In September 2020, a woman driving with her children stopped near Gujjarpura due to a lack of gasoline. She called a relative and texted him, her location on the highway. When the relative arrived, he noticed that the woman was upset and that there were bloodstains all over her clothing. Her vehicle's windows were also shattered and broken. The information of this case and salient points of judgment presented in Table 4.

Table 4: Facts of Motorway case

Sr#	Details	
1.	A women travelling on Motorway	
2.	Name of criminals	Abid Malhi and Shafqat Hussain
3.	City	Lahore
4.	Previous history	Robbery
5.	Modus operandi	Mischief, Robbery, Abduction by force, took the victim to jungle, Torture, gang raped in front of her children
6.	Chain of offences committed	Breaking car window glass, Abduction, captive (kept women and children in confinement), torturing, rapping, as well as for committing a terrorist act on road including robbery.
7.	Evidence	35 different evidence presented in court including the accused's confessional declaration, testimonies, oral proof, forensic evidence, DNA report, Mobile Data, geo-fencing record.
8.	Prominent Feature of case	Prosecution based the case on strong circumstantial and forensic evidence and confessional statements
9.	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
10.	Charges	Award of Punishment to both criminals
	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/-

The prosecution successfully contested each witness' evidence, correctly, appropriately, properly, suitably, and in accordance with legal procedure. This approach is also advantageous to the prosecution's case. After the decision of the case regarding rape of a woman on highway activated protests for publicly hanging the criminals. Prime Minister of Pakistan stated that the rapists must be chemically castrated.

5.3: Case Study 3:

Case regarding rape and killing a woman

The woman was found dead in a house in Lahore's DHA Phase V on May 3, 2021 Mayra Zulfiqar had come to Pakistan two months back and had been living with a friend in her house. She graduated from Middlesex University UK. Two men who wanted to marry her threatened her. According to Police investigation, the murder was committed, and confessed by murderers of a young girl, who was strangled and shot dead. Police had previously visited the area looking for CCTV of a car involved in the alleged abduction, according to residents on the upmarket street where Ms Zulfiqar was renting the upper portion of a house. On condition of anonymity, a neighbor told the BBC that loud arguments could often be heard from the property, and that men brandishing knives had been seen threatening Ms Mayra Zulfiqar on one occasion.

Table 5: Facts of Marya Zulfiqar case

Sr#	Details	
1.	Name of 26 years girl murdered	Mayra Zulfiqar Belgian Pakistani national living in London, Pakistani
2.	Name of Accused	Zahir Jadoon
3.	City	Lahore Punjab
4.	Previous history	Personal hostility
5.	Modus operandi	Threated to kill earlier, Abduction, criminal had intoxicated Maryra, had a scuffle, fight and brawl with her. She was strangled, shot and Murdered
6.	Offences committed:	House breaking, intoxication, torturing, rapping, and killing; as well as for committing a terrorist attack
7.	Evidence	The accused's confessional declaration, testimonies, oral proof,
8.	Prominent Feature of case	Prosecution based the case on strong circumstantial and forensic evidence
9.	Punishments:	Case pending for trial/decision.

5.4: Case study 4

Harassment and Sexual terrorism on a woman by 400 men

According [19] and [20], a demoralizing and heart touching incident occurred in Lahore while people were celebrating the Independence Day on 14thAugust 2021 at Miner-e-Pakistan, where adequate security was not engaged. A woman was taking snaps and filming, wearing green respectable dress with her colleagues and a camera operator. A big group of 400 people attacked her camera operator and 5 colleagues, snatched the camera, took away her ornament and purse containing cash. She was severely and harshly beaten and repeatedly thrown upward in air. The entire nation is sad on the manner; she was assaulted and harassed. The innocent women was Tortured, Intimidated and Harassed for more than 3 hours. The FIR is registered. The case can be traced and identified by using geo-fencing, CCTV footages and videos prepared by other people shared on social media in the gathering and volunteer eyewitnesses. The identities of the offenders can be traced, using their images from NADRA's Database. The Police is using the forensic and digital forensic techniques to trace the mobile numbers and identities of persons available at that time in the gathering. The images of people are clear and identified. The incident has elicited strong reactions from the public. The incident was described as "shameful" and "disgusting", by political leaders and human rights activists. People have demanded that the perpetrators be apprehended as soon as possible, and have questioned the government's policies for protecting women from assaults.

Table 6: Facts of Mina-e-Pakistan Case

Sr#	Details	
1.	Name of Victim	Miss Ayesha Akram
2.	Number of alleged offenders	400 unidentified persons, as per FIR
3.	City	Lahore Punjab
4.	Previous history	No personal hostility

5.	Modus operandi	Attacking a women, making her naked publically, insulting , assaulting , harassing, Theft of gold earrings, camera and cash, Torturing by throwing her upward multiple number of times, kept her udder threat to kill as she was fainted during the scuffle, fight and brawl with innocent woman
6.	Offences committed shown in FIR	Torturing, committing a terrorist attack, threat to kill, assaulting , harassing Sections 354-A (assault or use of criminal force against woman and stripping her of her clothes) Section 382 (theft after preparation made for causing death, hurt or restraint in order to commit the theft), Section 147 (rioting) Section 149 (unlawful assembly) of the Pakistan Penal Code.
7.	Present status of the case	Case pending for investigation under strong and non-bailable clauses

5.5: Illustration

The above case studies clearly show that the success of the every criminal case depends upon the careful investigation; collection of relevant evidence; witnesses and other types of evidence listed in Table 1 and organized tactfully to strengthen the hands of the prosecution leads to right direction in the court of Law. In the Multidimensional crime there may be long linked list of occurrences of crimes to commit target offence, for, example, murder; Table 5 shows such a linked list. It is not necessary that all the following offences must exist at a time, but a combination or a permutation may exist to formulate a multidimensional crime. For example, a man may kill another person first attempting abduction by persuasion, ask for and gets ransom money, keep in confinement in a solitary place for some time, inflict extensive torture and ultimately execute the killing.

Table 7: Illustration of multidimensional offences in case of Murder

Narcotics addiction	Mischief	Abduction by persuasion	Abduction by force	Robbery	Torturing	Child abuse
Harassment to women	Sexual Violence	Causing serious injuries	Zina	Rape	Attempt to murder	Murder

5.6: Significance of confessional statement

Confession is the admission of guilt, or the stating or implying of guilt, by an accused person while in custody. A "confession," according to Justice Stephen, is an admission made at any time by a person charged with a crime stating or implying that he committed the crime. The commentary on the confessional statement and its recording under section 164 and 364, 533, Cr.P.C, available in [18]. According to Lord Macaulay [18], words may easily be misunderstood by an honest man," says one expert. Knave could easily misinterpret them. What was said in a metaphorical sense could be taken literally. What was said ironically could be taken seriously. A participle, a tense, a mood, or an emphasis could mean the difference between guilt and innocence. Section 5A makes it mandatory for the Magistrate to record the prosecutrix's

statement under Section 164(5A) of the CrPC. As soon as the crime is brought to the officer's attention, he is obligated to take the victim to the nearest Judicial Magistrate to have his/her statement recorded. Section 164 of the code gives power to the Metropolitan Magistrate or judicial magistrate to record confession and statements during the course of investigation under chapter 12 or under any law for the time being in force, or at any time afterwards before the commencement of the inquiry or trial.

Procedure for Recording Confessional Statement

The Magistrate must ask following prescribed questions before recoding a confessional statement:

Table 8: Mandatory Questions asked before recording confessional statement

Sr#	Questions
1.	How long have you been with the Police?
2.	Has any pressure been brought to bear upon you to make a confession?
3.	Have you been threatened to make a confession?
4.	Has any inducement been given to you?
5.	Have you been told that you will be made an approver?
6.	Why are you making this confession?

6. The Important Ingredients of Forensic Reports

There are several element and aspects of the forensic and digital forensic reports depending upon the nature of offences committed For example, if rape is committed prior to killing the petitioner (victim); then offence proved by means of matching DNA report. The recovery of sharp edged weapon used for torture with bloodstains and the fingerprints on the weapon are relevant and of extremely important in investigation and prosecution both in the trial. The weapon recovered can be used to determine the brutality during course of offence. Digital forensic science is a branch of forensic science that focuses on recovering and investigating data from digital devices used in crime. The sources of information may be computers, personal Mobile, PDAs CCTV footages. Fingerprints and DNA are more highly distinguishing forensic evidence. Forensic evidence is "always trustworthy, establishes the elements of a crime. In case of death of the victim / (woman)**, the "Post Mortem Report"** is most significant document to determine the cause of death and provides evidence if rape was committed.

Table 9 : Important points to remember in Evidence preparation:

Collection	**preservation**	**Identification**	**extraction**	**documentation**
Validation	**Analysis**	**Interpretation**	**Evidence Assessment**	**Evidence Examination**
Evidence Acquisition	**Fingerprints**	**Blood**	**Blood stains**	**semen stains**
Drugs and Alcohol	**DNA test**	**Hairs**	**Fibers**	**Toolmarks**
Messages	**Images,**	**Videos**	**Sd cards**	**Call logs**

Table 10: Crime Statistics of Punjab (January-July 2021)

Sr#	Crimes	Number
1.	Abduction of women	6954
2.	Rape and Zina	1890
3.	Child Abuse	752
Note: Maximum cases reported at Lahore		

7. Why Attacks and Torture on Innocent Children and Women?

Children are tortured, abused, raped, molested, and killed in religious schools and their associated hostels. Police recently arrested a "private school" instructor who was flogging and lashing innocent children under the age of seven with a long rubber pipe for forgetting their lessons. School sticks inflict serious wounds on the delicate bodies of children. Criminal have psychiatric problems and disorders. The major reasons are absence of any deterrence force of Law or Police, which can prohibit offenders. Police is silent spectator most of the times. Poverty, delay in young male marriages, unemployment, projection of nude and pornographic material and video on social media, and films.

8. Recommendations:

1. The investigation of the criminal cases where forensic science is helpful, the modern techniques be applied, using information technology, roaming information stored on the telephone and service provider end, the addresses of the travelling offenders can be identified.

2. The Prosecution may rely for successful results, on forensic and digital forensic evidence collected and presented properly for court proceedings as demonstrated in study case 1 and 2 above.

3. Easily trace the forensic data retrieved from mobile messages and other necessary information about the offenders' mobile phones and laptops, such as messages, images, videos, SD cards, and call logs.

4. Enforcement of strict laws is the need of day. Owing to non-reporting of incidents, the real figures are exceptionally high.

5. Federal authorities must prohibit domestic child and women abuse and torture during labor.

6. Torture and abuse of orphan children studying and staying at religious schools by instructors must be looked into its real existence and offender punished.

7. Mufi Abdul Qavi ,who was arrested and nominated in the murder of a girl Qandeel Baloach was set free.

8. The case of Mufi Aziz-ur-Rehaman is a test case for exemplary punishment, no clemency, mercy or leniency be extended to him.

9. The death penalty be imposed where (as provided in Law) and criminals proved guilty by courts; the death penalty, according to public demand; be exercised publically in cases of horrible, heinous, unlawful, dreadful, scandalous, and wicked offences committed against innocent women and children.

10. The rapists must be chemically castrated

as desired by Prime Minister or publicly executed as per law,

11. The terrorist attacks committed by certain criminals against innocent women and children and civilians, as discussed in the above study cases be punished with death penalty, in accordance with law. "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," says Attorney General Eric Holder.

12. 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.

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]: Aftab Ahmad Malik, Waqar Azeem, Mujtaba Asad (2021) , " Requirement of strong legal frame work and procedures to contest with Cybercrime in Pandemic Situation , International Journal for Electronic Crimes Investigation"(IJECI) Volume 5, Issue 1 ; PP:03-12.

[2]: Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2020), "To Combat White Collar Crimes in Public and Private Sector and Need for Strong Legislation and Ethics", International Journal for Electronic Crimes Investigation"(IJECI); Vol 4 Issue 3, July-September PP:1-8.

[3]: Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2020), Importance of Prosecution Witnesses in Terrible Crimes of Sexual Violence, Abduction, Abuse, Torture, Rape and Killing against Innocent Women And Children Volume 4 , issue 4 PP: 03-14 , International Journal for Electronic Crimes Investigation"(IJECI) ISSN 2522-3429.

[4]: 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"(I-JECI) Published in Volume 4 issue 2, April-June ; PP 1-10

[5]: Dr Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2020), "Standardization of forensic evidence its procurement preservation and presentation in court of using FBI techniques by FIA"; International Journal for Electronic Crimes Investigation (IJECI); Published Volume 4 issue 1 , Jan - March :PP :1-6.

[6]: Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem (2019), "Deficiencies In PECA and Proposed amendments to facilitate Investigating Agencies, Courts and Prosecution, Proper Use Of Electronic Devices For Effective Implementation Of Law"; "International Journal for Electronic Crimes Investigation"(IJECI) Published in October-December Issue.

[7]: Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem (2019), "Bank Frauds Using Digital Devices and the Role of Business Ethics", "International Journal for Electronic Crimes Investigation"(I-JECI) volume 2 issue 4.

[8]: Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem (2019), "Electronic Devices to Investigate Offences of Torturing, Abusing, Molesting Assaulting or Killing the Innocent Children"; Published in International Journal of Electronic Crime Investigation (IJECI); Volume 3, issue 2; April-June.

[9]: Aftab Ahmad Malik , Mujtaba Asad, Waqar Azeem (2018, "Effective Prosecution To Support Digital Forensic Evidence During Investigation And Court Proceedings", International Journal for Electronic Crime investigation, ISSN 2522-3429;IJECI; Volume 3, Issue :1 , April-June.

[10]: Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2018): "Procuring Confessional Evidence of Criminals, Its Significance as Compared to Forensic, Digital and Other Oral Evidence of Witnesses"; LGU International Journal for Electronic Crime Investigation; ISSN 2522-3429;IJECI; Volume 2(3) July-September ; PP 01-08.

[11]: Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem(2018), "DNA Fingerprints, Facial Prints and other Digital Forensics as Evidence in Criminal Investigation and Court Proceedings", International Journal for Electronic Crime investigation, ISSN 2522-3429;I-JECI; Volume 2, Issue :1 ,PP 01-09; January-March.

[12]: Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2018), "Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed, International journal for electronic crime investigation, ISSN 2522-3429 ; IJECI ; Volume 1, Issue :1 , October-December

[13]: Jess Scherman (2019),"Types of Evidence You May Encounter as a Paralegal" https://www.rasmussen.edu/-degrees/justice-studies/blog/types-of-evidence/

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

[15]: Quran: Sura Al-Noor verse 2, 4 and 5.

[16]: Javaid Rehman, Eleni Polymenopoulou (2013), "Is Green a Part of the Rainbow? Sharia, Homosexuality and LGBT Rights in the Muslim World", Fordham International Law Journal Volume 37, Issue 1 2013 Article 7

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

[18]: https://blog.ipleaders.in/recording-of-statement-under-section-164-crpc/

[19]: https://www.dawn.com/news/1641385

[20]: https://www.samaa.tv/news/2021/08/minar-e-pakistan-incident-fir-registered-against-400-men-for-harassing-attacking-woman/

Iqbal *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. 5 issue 3 Year 2021

Communication Mechanism in a Distributed System

Zain Ali, Sehar Afzal
University of Lahore
Zainali114@gmail.com
seharAfzal43@gmail.com

Abstract:

In this research, problems are discussed dynamically distributed systems that relate to the sharing of data and communication from one system to another over the network. A distributed system communicates with its related systems by sending and receiving messages over the internet and in this way, it fulfills its work. When we discuss dynamic distributed systems, it means that it includes many different changeable types of networks, different operating systems like android, mac, windows, different software processors portability, breaking down of WAN, and inter-process communication errors. Another problem that accrues in distributed systems is latency. So, it is very difficult to develop software for these types of environments. Proposed work is related to make message communication in distributed systems easy, reliable, and efficient. For the sharing of data, coherence is responsible. Every problem can be solved but that proper

appropriate methods and algorithms are required. We create a new method which is a dynamic atomic shared memory for message communication. A properly stated method is proposed for message communication and then implemented. According to this method, owners can be changed dynamically and their access to read and write also changes.

1. Introduction

In this research, problems are discussed dynamically distributed systems that relate to the sharing of data and communication from one system to another over the network. A distributed system communicates with its related systems by sending and receiving messages over the internet and in this way, it fulfills its work. When we discuss dynamic distributed systems then it means that it includes many different changeable types of networks, different operating systems like android, mac, windows, different software processors portability, breaking down of WAN, and inter-process communication errors. The communication mechanism in distributed systems is related to how the system sends and receives messages from one system to another over the internet. In distributed systems, multiple systems relate to each other's, so a specific and well-defined method is required

for efficient and accurate communication. To fulfill this purpose, we developed a method which insured the accuracy and reliability of communication in processes. The focus of this work is to gain favorable results and assuring of communication and it helps to develop application easier. The reliability provides a guarantee about communication and coherence provides a guarantee about the sharing of data. Algorithms results are checked at lower bound to explain the limitations and cost of problems that can be faced. We create a new method which is a dynamic atomic shared memory for message communication. A properly stated method is proposed for message communication and then implemented. According to this method, owners can be changed dynamically and their access to read and write also changed. In this proposed work, we provide the best solution for implementation for communications in dynamic distributed systems that avoid crashes. Its performance in evaluates timing and failure of communication.

2. Literature Review

In the past, work is done for the inquiry of a lot of complications, errors and duplication of data on distributed algorithms [6,7], and group membership and communication mechanisms are checked [5,8]. We also focused on the previously implemented studies [3, 13]. A lot of mechanisms are used in different academic and commercial systems for communication in processes. They act as a middleware for the process to process communication in distributed systems. Mostly they used in group communication distributed systems [4]. An inspirational work which helps to develop this work is atomic data from dynamic voting systems [15] protocols. This system can manage a lot of processors in distributed systems [14]. To handle the problems just like inconsistency in the breakdown of communications in processes, and some are used to demand the systems for configuration. It is noticed that it is very useful for problem detection and generates solutions for these problems. From recent studies and it is noticed that algorithms are very complex which are developed to detect the problems and errors in distributed systems. Such algorithms help a lot to decrease the complexity by using global services with good interface and practices. An example of this conscious algorithm which provides a baseline for other related works [9]. To check the performance and efficiency of this algorithm, decomposition is used.

3. Problem Statement:

Dynamic Distributed Systems

For data sharing and communication problems in dynamic distributed systems, we are focusing new direction. The environment will be less interacting for example an unlimited number of processors, Request from the user to join and leave the system. Our purpose is for coherent theory and we see service for the lower bound and upper bound algorithm results. With the passage of time, the number of processes and their connections is changed over a network. Processors can be added, recover if they fail in a network. Processors can be connected via mobile and wirelessly. An application may move from one place to another, on these conditions we will consider distributed running application which has identification and information of users include file, multimedia, real-world information, and

games.

4. Approach

As the high-level global services are solved, communication and data sharing problems are solved in the same way. According to the environmental performance expectation, these

services maintain the problems and fault tolerance.

Research on distributed services focuses on correctness, On the other hand, Algorithm focuses on performance. Our work will combine these two techniques which will produce algorithms that work efficiently will break down in dynamic distributed systems then performance and fault tolerance squeeze out by global services. We will include a balanced study of performance and service assurance. Atomicity is expensive so resolve consistency which may reduce the cost and will provide benefits.

The setting of these techniques is difficult, so it is also difficult to develop these algorithms which means that we have to break down bigger pieces into smaller pieces. These pieces will be viewed as lower-level global services. These services will provide data sharing and lower-level communication for example resource allocation, routing, failure, and progress detection. These services also include fault tolerance and performance which can be repeated again and again. The work we focus to achieve goals are given below:

-State new services focus on communication and data sharing in a Distributed environment

- Developing and analyzing an algorithm in a dynamic system to implement these services

This work is achieved by the mathematical framework based on state machines which include the feature to convey timing issues, behavior, and probabilistic behavior. Give assistance to Meta theory include models, measure performance and analysis proof methods will also be developed. Our theoretical work contributes features to the implementation and testing of distributed systems services. This work is conducted by examples that are selected from file management, application prototype, collected information, games, and computer cooperative work. During developing the specification for the system, we also focus on the developer's opinion and information for service assurance.

5. Atomic Memory Service

Reconfigurable memory service on the algorithm for a distributed system that can be used to reading and writing memory in a dynamic network [12]. Users can join and leave during the action of mathematical calculation. Examples are mobile and peer computing networks. The benefit of this service is that data can survive for a long time in a dynamic setting.

We identify and introduce atomic memory serves as a global service called RAMBO means Reconfigurable atomic memory for basic objects. Dynamic distributed algorithms implement this global service. To obtain presence objects are reproduce and also to

obtain repetition in the availability of small changes algorithm use configuration which includes read and write sets of belonging struc-

ture. To provide large and small changes algorithms use reconfiguration in which members are updated. These types of updates do not use any infraction and objects configuration can install any time.

The algorithm includes major actions like reading, writing, configuration, and out of date configuration. Algorithm merge in the main algorithm which handles garbage collection and global reconfiguration services. Reconnoiter provide the main algorithm to repeat configuration. Reconfiguration does not fir tightly in the main algorithm. The major configuration may be used one time but read and write use them all the time.

The main algorithm performs read and write operations. Information collected from reading operations and spread information from writing operations. Both operation use for active configuration. This communication put into the background which allows the algorithm to maintain information. Every stage is finished by a condition that includes objects from the configuration. Read and write actions may run simultaneously. Garbage collection is used when there is no type of configuration used for repetition.

Reconfiguration service is executed by a distributed algorithm that involves a general agreement to configuration. An object from a new configuration may introduce a new configuration, many invitations are consistent by running general agreement among objects. General agreement executed by the Paxos algorithm [11]. That type of general agreement is slow but in some condition may not be finished but they do not read and write action slowly.

Garbage collection uses two stages in which the first stage communicates with old configuration and the second stage communicates with the new configuration. Garbage collection action makes surety that objects of reading and writing old configuration learn new configuration.

We evaluate performance based on time and failure action means garbage collection occurs from time to time, reconfiguration is requested for garbage collection to keep up, objects of active configuration do not fail, then we show that read and write action perform in maximum latency time.

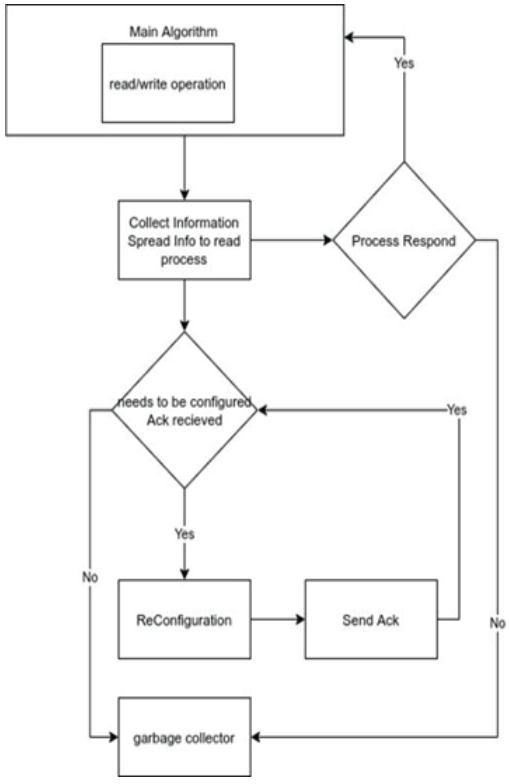


Figure 1

Our proposed method is to overcome problems found in the previous literature that is PAXOS algorithm used for the process to process

communication and when the failure of one process occurs it disturbs Communication. Global service called RAMBO Reconfigurable atomic memory for basic objects. Dynamic distributed algorithms implement this global service. Our method includes major action like reading writing, configuration, and reconfigure

out of date configuration as we can see in figure 1.The first step includes the Algorithm merge in the main algorithm. The main Algorithm handles garbage collection and the global reconfiguration services in the main algorithm perform read and write operation. Information collected from reading operations and spread information to writing operations. Both operation use for active configuration. This communication put into the background which allows the algorithm to maintain information. Every stage is finished by a condition that includes objects from the configuration. Read and write actions may run simultaneously. Garbage collection is used when there is no type of configuration used for repetition.

6. Conclusion

Our proposed work is different from other works because it acts as a middleware in communication in distributed systems. There are a lot of different frameworks such as CORBA, DCE, and Java/JIN which are used to develop different distributed systems. But they have small scope according to their components, their specification, and architecture according to their formal definition and informally from their behavior. By using these methods and services, the performance of dynamic distributed systems cannot be supported by these frameworks. On the other hand, our proposed work is very helpful to provide initial help to handle the faults and errors during communications. This proposed work is best because its interface and behavior are accurately elaborated. The performance and fault tolerance for communication in distributed systems are mentioned in the behavior of an algorithm. The reliability, accuracy, error detection and handling, and performance can be handled by our proposed method because it handles it during its computation.

We are assuring that our proposed work will be very helpful in the theory of algorithms construction. It will provide the analysis for complications accrue during communication in dynamic distributed systems. It will provide as much strong communication and accuracy as available in static distributed systems. This project is based on the theoretical. To develop the dynamic distributed systems, our algorithm and framework are very strong to ensure the accuracy and performance of systems. Some additional work is required just like ours into systems for some other purpose. It is as same as components that are created by the help of object-oriented and component technologies in software engineering [2].

7. References:

[1] H. Attiya, A. Bar-Noy and D. Dolev, “Sharing Memory Robustly in Message-Passing Systems", J. of the ACM, vol. 42, no. 1, pp. 124-142, 1996.

[2] Kenneth P. Birman. A review of experiences with reliable multicast. Software, Practice, and Experience, 29(9):741–774, September 1999.

[3] O. Chenier and A. Shvartsman, “Implementing an eventually-serializable data service as a distributed system building block,” in Networks in Distributed Computing, vol. 45, pp. 43–72, AMS.

[4] Communications of the ACM, special section on group communications, vol. 39, no. 4, 1996.

[5] R. De Prisco, A. Fekete, N. Lynch, and A. Shvartsman, “A dynamic primary configuration group communication service,” in Distributed Computing Proceedings of DISC’99

- 13th International Symposium on Distributed Computing, 1999, LNCS, vol. 1693, pp. 64–78.

[6] B. Englert and A. Shvartsman. Graceful quorum reconfiguration in a robust emulation of shared memory. In Proc. of the 20th IEEE Intl Conference on Distributed Computing Systems (ICDCS’2000), pp. 454-463, 2000.

[7] A. Fekete, D. Gupta, V. Luchangco, N. Lynch, and A. Shvartsman, “Eventually-serializable data service,” Theoretical Computer Science, vol. 220, no. 1, pp. 113–156, June 1999.

[8] A. Fekete, N. Lynch, and A. Shvartsman. “Specifying and using a partitionable group communication service." ACM Trans. on Computer Systems. vol. 19, no. 2, pp. 171-216, 2001.

[9] R. Guerraoui and A. Schiper, “The Generic Consensus Service," IEEE Trans. on Software Engineering, Vol. 27, No. 1, pp. 29-41, January 2001.

[10] S. Haldar and P. Vita´nyi, “Bounded Concurrent Timestamp Systems Using Vector Clocks", J. of the ACM, Vol. 249, No. 1, pp. 101-126, January 2002

[11] Leslie Lamport, "The Part-Time Parliament", ACM Transactions on Computer Systems, 16(2) 133-169, 1998.

[12] N. Lynch and A. Shvartsman, “RAMBO: A Reconfigurable Atomic Memory Service", in Proc. of 16th Int-l Symposium on Distributed Computing, DISC’2002, pp. 173-190, 2002.

[13] K. W. Ingols, “Availability study of dynamic voting algorithms,” M.S. thesis, Dept. of Electrical Engineering and Computer Science, MIT, May 2000.

[14] M. Merritt and G. Taubenfeld, “Computing with infinitely many processes (under assumptions on concurrency and participation),” In Proc.14th International Symposium on DIS- tributed Computing (DISC), October 2000.

[15] E. Yeger Lotem, I. Keidar, and D. Dolev. “Dynamic voting for consistent primary components." In Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing, pages 63–71, August 1997.

Umar *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. 5 issue 3 Year 2021

Optimal Query Execution Plan with Deep Reinforcement Learning

Umar Jamshid1, Muhammad Umar Afzal[2]
umer.khokher@gmail.com1 umar.afzl@ymail.com[2]
University of Lahore

Abstract:

We examine the use of profound support learning for inquiry development. The technique is to gradually construct queries by encoding features of sub-inquiries using a learnt representation. We specifically focus on the organization of the state progress effort and the state portrayal issue. We provide preliminary results and investigate how we might use the state representation to further refine question streamlining using assist learning.

1. Introduction

Inquiry advancement is still a big concern in the field of data sets. Existing DBMS select helpless execution strategies for certain queries. To make inquiries more competent, we wished to design them optimally, utilizing fewer assets. Existing DBMSs carry out a vital stage of cardinality evaluation by working on assumptions about the information (e.g., incorporation standard, consistency or freedom suppositions). When these concerns are not confirmed, cardinality evaluation errors occur, resulting in poor arrangement choices. [1]. By using cardinality gauges as input, the expenditure model selects the least expensive alternative from semantically equivalent arrangement options. To achieve an efficient inquiry strategy, a subset of the valid join orders is counted by the question enhancer, for example, using dynamic programming.

Theoretically this architecture can obtain the effective optimal plan if the cardinality estimation and cost model is precise. In reality cardinality estimates depends on computer-based assumptions. But in real world databases the assumptions like uniformity and independence are wrong.

In this research work, rather than banking on previously used formulas and data driven with the help of statistics, to predict the queries cardinalities we will train a deep reinforcement learning model for better execution plan. We will construct a model that can learn data and

properties of data to be exact about the estimates. The major part of this model is that it will learn the subquery representations of complex queries which will be used to build query execution plan using deep reinforcement learning. Since the 1970s, information base analysts have been dealing with framework enhancement and large-scale information-driven applications, which are strongly associated with the first two components. Although deep learning methodologies are not often used in dealing with DBMS challenges, it is natural to wonder about the linkages between information bases and profound learning.

First, we have to examine that is the database community ready to adapt deep learning for DBMS. However, there are fewer examples of using machine learning for traditional database problems that are less uncertain, like indexing etc. whereas deep learning is good at predicting the events that are mostly contains uncertainty. There are problems faced in databases that are probabilistic like crowdsourcing etc. In particular, we divide the method in two parts, first representation of state of table using deep learning and then we will present a way to computes plan for the given query using the above states together with deep reinforcement learning.

Challenge of this approach, to represent data and query. First, we develop an approach that will incrementally generate result of subqueries. Subqueries and a new operation will be provided as input that will further predict the representation of output. This representation of output subquery will be used to derive the subquery's cardinality.

The major part is that we will present a method that will use this representation to enumerates the query execution plan through deep reinforcement learning. Support learning is a generally beneficial structure used for dynamic in circumstances where a framework is absorbed by experimentation from remunerations and discipline. [2]. We propose to use this deep learning approach to build an optimal query execution plan by modelling it as Markov process; in which each decision has its dependency on each stage. The figure below will illustrate our method. The figure below has DB and a query, the model will generate an optimal query execution plan by determining the series of state transitions

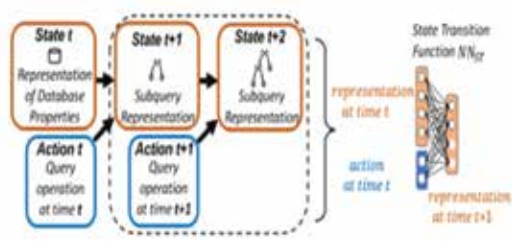


Figure 1: Database System

The system in the initial state t in the illustration represents a whole database. We will select as action using deep reinforcement learning, the model moves to a new state at **t +1**, We've now built a bigger subquery. Each action is a query operation, and each state reflects the intermediate results of the subquery. To build this representation, we used a neural network, i.e. a state transition function, NNST. NNST is a recursive function that generates the subquery representation at time

t+1 by taking the previous subquery representation as input and an action at time t.

Let us now define the setup that is engineered above. The query plan's dynamics are bottom-up, with one operation at a time. Assume a subquery has been constructed at any step t of the query plan, and the state at t is represented by an n-dimensional vector h_t. When the next action applied to the setup, at to this current database state leads to the next state, ht+1. The mapping, $\mathbf{NN_{ST}: (h_t, a_t) \rightarrow h_t+1}$ is called the state transition function. This state and state transition function are well known in applications of deep reinforcement learning. For Example, in the game of Chess, each possible position is called state and the transition of these states from one board position to another is well-defined. However, in the case of a database, if the query execution plan is not sufficiently described, we cannot forecast the status of the query. The core of our proposed strategy is to identify each state using a finite dimensional vector and then learn the state transition function using a deep reinforcement learning model. We employ input signals and context from observed variables linked with database status to drive the training procedure for this network. Throughout this work, we will utilise the cardinality of each subquery as an observable variable at any point of the plan. If we can learn a function, $NN_{observed}$, that maps this state to projected cardinalities at stage t, we should be able to learn a function, $NN_{observed}$, that maps this state to predicted cardinalities at stage t. In the figure below, we display both NNST and $NN_{observed}$.

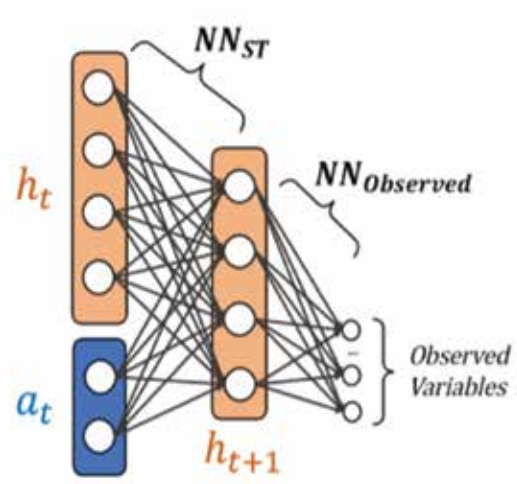


Figure 2: Representation of NN_{ST} and $NN_{Obsereved}$

When the suggested model has been sufficiently trained, we will update the network parameters depending on query operation sequences. Each state will learn to precisely depict a representation using this approach. Once the technique has been fully trained, we may correct it and use deep reinforcement learning to create a suitable action policy, resulting in an optimal query execution plan.

2. Literature Review:

Extensive Learning Deep learning methods, commonly known as feedforward neural networks, may imprecisely approximate a nonlinear function, f [3]. Through a collection of learnt parameters spread across multiple layers, these models establish a mapping from an input x to an output y. The behavior of the interior layers is not dictated by the input data during training; instead, these models must learn how to employ the layers to create the proper output. Because the layers have no

direct interactions with the input training data, they are referred to as hidden layers [3]. These feedforward networks are crucial in representation learning. While training to perform a goal function, the hidden layers of a neural network might indirectly learn a representation that can later be employed for other tasks [3]. There is a trade-off between retaining as much information as possible and understanding relevant data qualities. The context of these representations might alter depending on the network output [3]. Learning through Reinforcement learning models can map states to appropriate actions with the objective of maximizing a larger reward. In contrast to supervised learning, the learner is not clearly informed which action is ideal; instead, the agent must determine the best action through hit-and-run by either exploiting current information or finding novel states [11]. At each time step, the learner will examine the condition of the environment, S_T, and choose an action, a_t. The policy determines the action to be taken. This strategy has the potential to reconstruct a variety of behaviors. As a result, either behave greedily or strike a balance between discovering and utilizing through a greedy (or better) method. The policy is determined by the predicted rewards of each state, which the model must learn on the fly. The model will arrive at a new state, S_{T+1}, based on the action chosen. The environment then provides the agent a reward, r_{T+1}, signifying the "worthiness" of the chosen action. The goal of the agent is to maximize the overall reward [11]. One method is to employ a value-based iteration methodology in which the model records state-action values, such as QL (s, a). These values indicate the state's long-term worth by weighting rewards for states that are anticipated to follow.

3. Methodology:

They are two approaches that we proposed to achieve the target solution for getting the optimal query execution plan. We will be supposed input database ***D*** and Query ***Q.*** we will apply deep reinforcement learning to derive compact but informative representation of queries, then we will try to train these representations to predict the next action. In first approach we would suppose a feature vector containing (Q, D) as input and apply deep reinforcement learning to predict an output as cardinality values. There is problem with this approach that whenever the database and query complexity increase the input vector grow heavily. Thus, the long-extended vectors required large training datasets.

Instead of wasting our resources and never getting our required result, we will move forward and apply our better different approach, a recursive approach: We train a model to anticipate a query's cardinality. This model is fed a pair of (h_t, a_t) as input, where h_t is a vector representation of a subquery and a_t is a single relational action on h_t. Importantly, because h_t is the representation that the model will learn on its own, it should not be interpreted as a manually supplied feature vector. The NN_{ST} function, seen in the image above, builds these representations by modifying the weights in response to feedback from the $NN_{Observed}$ function. This $NN_{Observed}$ function learns to predict observed variables by mapping a

subquery representation. Back propagation is used to alter the weights for both functions while we train this model.

Before moving forward and start using the recursive NN_{ST} model, we have to understand an additional function, $\mathbf{NN_{init}}$. NN_{init} will take $\mathbf{(x_0, a_0)}$ as input, where x_0 represents a vector that holds the properties of the database D whereas a_0 shows a relational operator. The model outputs the cardinality of the query that executes the operation encoded in a_0 on D. By this we can achieve the optimal time on the execution of the query.

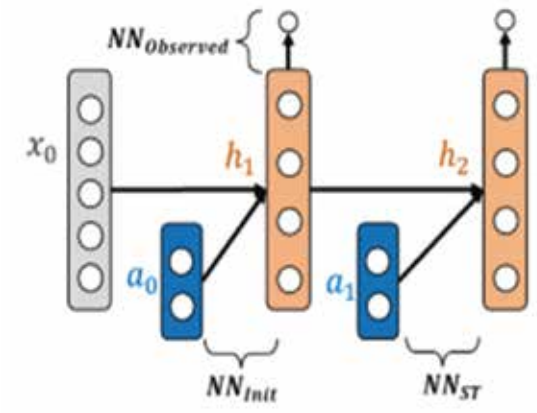
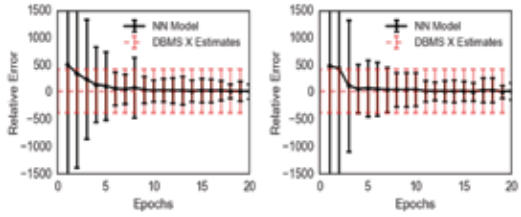


Figure 3: Input and Output Variables

x_0 the vector represents simple properties of the database, D. For each attribute in the dataset D, we use the following features to define x_0: ***the min value***, ***the max value*** and ***the number of distinct values***.

4. Conclusion

In this paper, we provide a model for query optimization that uses deep reinforcement learning. We employ deep neural networks to gradually learn state representations of subqueries by storing fundamental information about the input. In future work, we propose combining these state representations with a reinforcement learning model to develop optimum plans.



(a) Predicting Cardinality (m = 3) **(b) Predicting Cardinality (m = 5)**

5. References:

[1] Kostas Tzoumas et al. A reinforcement learning approach for adaptive query processing. In A DB Technical Report, 2008.

[2] Ron Avnur et al. Eddies: Continuously adaptive query processing. SIGMOD Record, 2000.

[3] Volodymyr Mnih et al. Human-level control through deep reinforcement learning. Nature, 2015.

[4] Viktor Leis, Andrey Gubichev. How Good Are Query Optimizers, Really? CoRR, 2017.

[5] Richard S. Sutton et al. Reinforcement learning I: Introduction, 2016.

[6] Wei Wang†, Meihui Zhang et al. Database Meets Deep Learning: Challenges and Opportunities. January 2020.

[7] Ryan Marcusetal. Deep reinforcement learning for join order enumeration. CoRR, 2018.

[8] Ian Goodfellow et al. Deep Learning. MIT Press, 2016. http://www.deeplearningbook.org.

[9] David Silver. UCL Course on Reinforcement Learning, 2015.

[10] Michael Stillger et al. Leo - db2's learning optimizer. In VLDB 2001.

[11] Viktor Leis et al. How good are query optimizers, really? Proc. VLDB Endow., 2015.

[12] Csaba Szepesvari. Algorithms for reinforcement learning. Morgan and Claypool Publishers, 2009.

[13] Martín Abadi et al. TensorFlow: Large-scale machine learning on heterogeneous systems, 2015. Software available from tensorflow.org.

[14] Wei Wang et al. Database Meets Deep Learning: Challenges and Opportunities. SIGMOD Record, 2016

[15] Henry Liu et al. Cardinality estimation using neural networks. In CASCON 2015

Shairoze *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. 5 issue 3 Year 2021

Machine Learning in Malware Detection

Muhammad Shairoze Malik*
13beemmalik@seecs.edu.pk
National University of Science
and Technology Islamabad

Abstract:

Malware has become one of the biggest cyber threats today with the rapid growth of the Internet. Malware can be referred to as any program that performs malicious acts, including data theft, espionage, etc. In a world of growing technology, protection should also increase at the same time. Machine learning has played a significant role in operating systems over the years. Cybersecurity is capable of using machine learning to boost organizations' detection of malware, triage, breach recognition and security alert. Machine learning will significantly change the cyber security climate. New techniques such as machine learning must be used to solve the rising malware problem. This paper aims to research how cybersecurity can be used for machine learning and how it can be used to detect malware. We will look at the PE (portable executable) headers of samples of malware and non-malware samples and create a classifier for malware that can detect whether or not malware is present.

Keywords: Cybersecurity, detection, malware, machine learning, PE headers, classifier, preparation, boost

1. Introduction

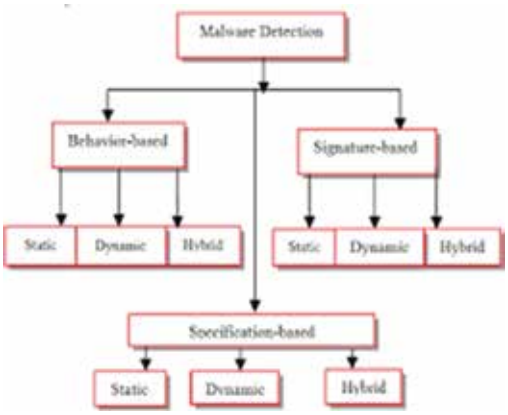
Idealistic hackers attacked computers in the early days because they were eager to prove themselves. Cracking machines, however is an industry in today's world. Despite recent improvements in software and computer hardware security, both in frequency and sophistication, attacks on computer systems have increased. Regrettably, there are major drawbacks to current methods for detecting and analyzing unknown code samples. The Internet is a critical part of our everyday lives today. On the internet, there are many services and they are rising daily as well. Numerous reports indicate that malware's effect is worsening at an alarming pace. Although malware diversity is growing, antivirus scanners are unable to fulfil security needs, resulting in attacks on millions of hosts. Around 65,63,145 different hosts were targeted, according to Kaspersky Labs, and in 2015, 40,00,000 unique malware artefacts were found. Juniper Research (2016), in particular, projected that by 2019 the cost of data breaches will rise to $2.1 trillion globally [1]. Current studies show that script-kiddies

are generating more and more attacks or are automated. To date, attacks on commercial and government organizations, such as ransomware and malware, continue to pose a significant threat and challenge. Such attacks can come in various ways and sizes. An enormous challenge is the ability of the global security community to develop and provide expertise in cybersecurity. There is widespread awareness of the global scarcity of cybersecurity and talent. Cybercrimes, such as financial fraud, child exploitation online and payment fraud, are so common that they demand international 24-hour response and collaboration between multi-national law enforcement agencies [2]. For single users and organizations, malware defense of computer systems is therefore one of the most critical cybersecurity activities, as even a single attack may result in compromised data and sufficient losses. This research explores how machine learning can be used in the field of cybersecurity, along with how it can be used to detect malware. In order to detect malware, we will examine the PE headers of malware and non-malware samples or files by creating and training a classifier that will determine whether the file has been attacked by malware or not after training.

2. Evolution of Malware

In order to protect networks and computer systems from attacks, the diversity, sophistication and availability of malicious software present enormous challenges. Malware is continually changing and challenges security researchers and scientists to strengthen their cyber defenses to keep pace. Owing to the use of polymorphic and metamorphic methods used to avoid detection and conceal its true intent, the prevalence of malware has increased. To mutate the code while keeping the original functionality intact, polymorphic malware uses a polymorphic engine. The two most common ways to conceal code are packaging and encryption [3]. Through one or more layers of compression, packers cover a program's real code. Then the unpacking routines restore the original code and execute it in memory at runtime. To make it harder for researchers to analyze the software, crypters encrypt and manipulate malware or part of its code. A crypter includes a stub that is used for malicious code encryption and decryption. Whenever it's propagated, metamorphic malware rewrites the code to an equivalent. Multiple transformation techniques, including but not limited to, register renaming, code permutation, code expansion, code shrinking and insertion of garbage code, can be used by malware authors. The combination of the above techniques resulted in increasingly increasing quantities of malware, making time-consuming, expensive and more complicated forensic investigations of malware cases. There are some issues with conventional antivirus solutions that rely on signature-based and heuristic/behavioral methods. A signature is a unique feature or collection of features that like a fingerprint, uniquely differentiates an executable. Signature-based approaches are unable to identify unknown types of malware, however. Security researchers suggested behavior-based detection to overcome these problems, which analyses the features and behavior of the file to decide whether it is indeed malware, although it may take some time to search and evaluate. Researchers have

begun implementing machine learning to supplement their solutions in order to solve the previous drawbacks of conventional antivirus engines and keep pace with new attacks and variants, as machine learning is well suited for processing large quantities of data. [4]



3. Malware Detection

In such a way, hackers present malware aimed at persuading people to install it. As it seems legal, users also do not know what the program is. Usually, we install it thinking that it is secure, but on the contrary, it's a major threat. That's how the malware gets into your system. When on the screen, it disperses and hides in numerous files, making it very difficult to identify. In order to access and record personal or useful information, it may connect directly to the operating system and start encrypting it [5]. Detection of malware is defined as the search process for malware files and directories. There are several tools and methods available to detect malware that make it efficient and reliable. Some of the general strategies for malware detection are:

i. Signature-based

ii. Heuristic Analysis

iii. Anti-malware Software

iv. Sandbox

Several classifiers have been implemented, such as linear classifiers (logistic regression, naive Bayes classifier), support for vector machinery, neural networks, random forests, etc.

Through both static and dynamic analysis, malware can be identified by:

✓ Without Executing the code

✓ Behavioral Analysis

4. Need for Machine Learning in Malware Detection

Machine learning has created a drastic change in many industries, including cybersecurity, over the last decade. Among cybersecurity experts, there is a general belief that AI-powered anti-malware tools can help detect modern malware attacks and boost scanning engines. Proof of this belief is the number of studies on malware detection strategies that exploit machine learning reported in the last few years. The number of research papers released in 2018 is 7720, a 95 percent rise over 2015 and a 476 percent increase over 2010, according to Google Scholar,1. This rise in the number of studies is the product of several factors, including but not limited to the increase in publicly labelled malware feeds, the increase in computing capacity at the same time as its price decrease, and the evolution of

the field of machine learning, which has achieved ground-breaking success in a wide range of tasks such as computer vision and speech recognition [6]. Depending on the type of analysis, conventional machine learning methods can be categorized into two main categories, static and dynamic approaches. The primary difference between them is that static methods extract features from the static malware analysis, while dynamic methods extract features from the dynamic analysis. A third category may be considered, known as hybrid approaches. Hybrid methods incorporate elements of both static and dynamic analysis. In addition, learning features from raw inputs in diverse fields have outshone neural networks. The performance of neural networks in the malware domain is mirrored by recent developments in machine learning for cybersecurity. [6]

5. Detailed Design

Our paper workflow is divided into 3 sections.

- Describing the details: The dataset is imported and the different columns are discussed in the dataset.
- Data cleaning: The required steps are taken after examining the dataset so that the dataset can be cleaned and all the null values and columns of not much significance are removed so that they will not be of any concern in the training part.
- Data Training and Testing: When the information is transparent and ready for training, we spilled the information as a training dataset and testing dataset in an 80:20 ratios so that the data was spilled in an 80:20 ratios.

In this paper, as we try to achieve the highest accuracy, we use two algorithms to see which will give us better precision.

- Gradient Boost Classifier
- Random Forest Classifier

6. Algorithms

Gradient Boosting- Gradient boosting is a technique of machine learning which uses regression and classification problems that helps us generate a prediction model in the form of an ensemble of the weaker prediction models, usually decision trees. As other boosting techniques do it constructs the model in a phase-wise fashion and generalizes them by allowing an arbitrary differentiable loss function to be optimized. [7] For predictive model growth, gradient boosting is one of the most effective techniques. Gradient Boosting is teaching several models steadily, additively and sequentially. With gradients of loss function, gradient boosting takes place. What we strive to develop and maximize depends on a simple understanding of the loss function.

- In Gradient Boosting, three elements area feature for loss to be optimized or enhanced.
- A poor man who has learned to make predictions
- A supplementary model for incorporating disadvantaged students to minimize losses. [8][9]

It's important that we understand how the algorithm of Gradient Boost is implemented under the hood.

1. Calculate average of target label- We begin with a leaf that is the average value of the variable we want to forecast when solving regression problems. This leaf will be used in the procedural steps as a baseline to reach the correct solution.

2. Calculate the residuals- Calculating the residual with the proceeding formula.

   Residual = actual value – predicted value

3. Construct a decision tree- Next with the intention of predicting the residuals, we build a tree. In other words, a prediction of the residual value (not the desired label) will be found in every leaf. Any residuals will end up within the same leaf in the event that there are more residuals than leaves. We compute their average and position that inside the leaf when this happens.

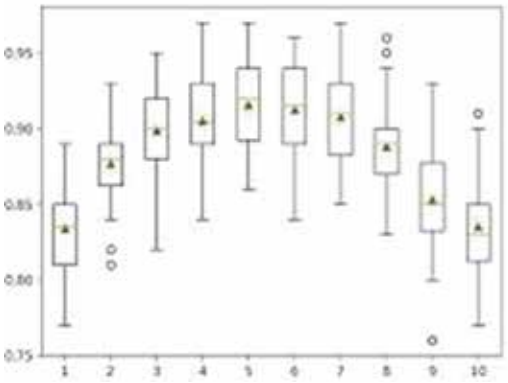
4. Using the trees within the ensemble predict the target label. - Each sample passes through the newly developed tree's decision nodes before it reaches a given lead.

5. Compute the new residuals- The residuals will then be used as explained in step 3 for the leaves of the coming next decision tree.

6. Repeat steps 3 to 5 until the number of iterations matches the number (i.e. the number of estimators) defined by the hyper parameter.

7. To make a final prediction as to the value of the target variable, use all the trees in the ensemble once eligible. [10]

In the first step, the final forecast will be equal to the mean we determined, plus all the residuals predicted by the trees that make up the forest multiplied by the learning rate.



Random forests - Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that function by constructing a multitude of decision trees at training time and generating the class that is the class mode (classification) or the individual trees' mean/average prediction (regression) of the individual trees. Random forests are often used as "Blackbox" models in companies, as they produce rational predictions over a large range of data while requiring little configuration in packages such as sci-kit-learn [11]. However, data characteristics can affect their performance. In the steps and diagrams below the working procedure can be explained:

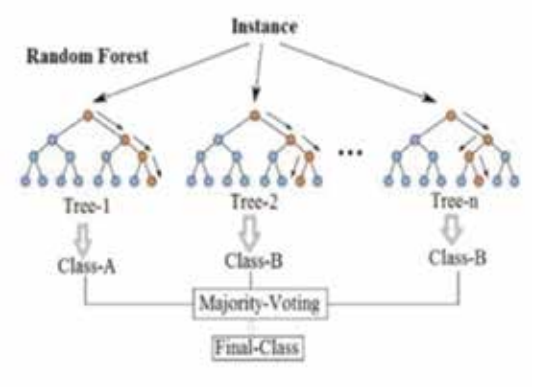
1. From the training set select random K data points.

2. Use the selected data points to build decision trees associated with it (Subsets).

3. Choose a number N which represents the decision trees that you want to build.

4. Repeat Step 1 & 2.

5. Find the predictions for new data points for each decision tree and assign the new data points to the group that receives the majority votes. [12]

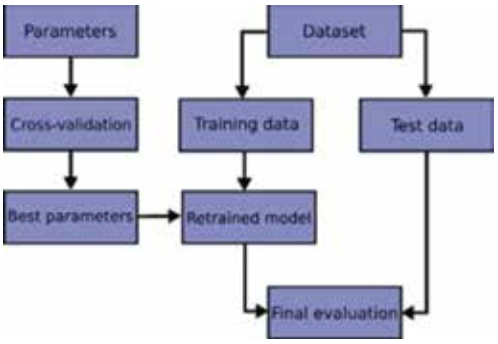


7. Mplementation

We used a dataset that was made available from the Chiheb Chebbi - Mastering Machine Learning for Penetration Testing book for this work. There are approximately 138000 entries of legit and malware PE headers and 56 columns as features in the dataset. In an 80 percent preparation and 20 percent evaluation, the knowledge was divided.

We initially import and read the dataset, once that is done, we clean the dataset by dropping unnecessary features and null values. After that we split the dataset for training and testing. We import the necessary packages for making a decision tree, gradient boosted classifier and random forest classifier. Once done we fit that data respectively and predict the results.

Using a combination of these algorithms, after training and testing the algorithms, we were able to get a highly accurate outcome.



8. Results

After training and testing both the algorithms, we can see that both of them give us a high accuracy output.

9. Conclusion

The algorithm used for training the data was Gradient Boosted classifier and random forest classifier which gives us an accuracy of 98.764% and 99.311% respectively. After viewing the confusion matrix of the random forest classifier, we could conclude that the number of false positives were at 0.5505 and false negatives were at 1.0053. And after viewing the confusion matrix of the Gradient boosted algorithm we can say that the number of false positives were at 0.768 and false negatives were at 2.3099.

Our main objective was to come up with a system for machine learning that typically detects as many samples of malware as possible, with the tough restriction of having a zero false positive rate. We have been really close to our target, but we still have a false positive rate that is non-zero. A variety of deterministic exemption mechanisms must be added in order for this system to become part of a highly competitive commercial product. In our view, machine learning detection of malware will not replace the existing methods of detection used by anti-virus vendors, but will come as an extension to them. Certain speed and memory limitations are placed on any commercial anti-virus product, so the most accurate algorithms should be used.

10. References

[1] Ahmadi etal., 2016. M. Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, G. Giacinto - Novel feature extraction, selection and fusion for effective malware family classification

[2] AL-Hawawreh etal., 2018 M. AL-Hawawreh, N. Moustafa, E. Sitnikova - Identification of malicious activities in industrial internet of things based on deep learning models

[3] Athiwaratkun etal., 2017 B. Athiwaratkun, J.W. Stokes - Malware classification with lstm and gru language models and a character- level cnn

[4] D. Bekerman, B. Shapira, L. Rokach, A. Bar - Unknown malware detection using network traffic classification 09 2015

[5] B. Biggio, F. Roli - Wild patterns: ten years after the rise of adversarial machine learning

[6] I. Santos, Y. K. Penya, J. Devesa, and P. G. Garcia, "N-grams- based file signatures for malware detection," 2009.

[7] K. Rieck, T. Holz, C. Willems, P. D¨ussel, and P. Laskov, "Learning and classification of malware behavior," in DIMVA '08: Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 108–125.

[8] E. Konstantinou, "Metamorphic virus: Analysis and detection," 2008, Technical Report RHUL-MA-2008-2, Search Security Award M.Sc. thesis, 93 pages.

[9] Gibert etal., 2019 D. Gibert, C. Mateu, J. Planes - A hierarchical convolutional neural network for malware classification. The International Joint Conference on Neural Networks 2019, IEEE (2019), pp. 1-8

[10] X. Guo, Y. Yin, C. Dong, G. Yang, G. Zhou - On the class imbalance problem 2008 Fourth International Conference on Natural Computation, vol. 4 (Oct 2008), pp. 192-201

[11] Hall, 1999 M.A. Hall - Correlation-based Feature Selection for Machine Learning Ph.D. thesis The University of Waikato (1999)

[12] W. Han, J. Xue, Y. Wang, L. Huang, Z. Kong, L. MaoMaldae: - Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics Comput. Secur., 83 (2019), pp. 208-233

[13] W. Han, J. Xue, Y. Wang, Z. Liu, Z. KongMalinsight: a systematic profiling-based malware detection framework J. Netw. Comput. Appl., 125 (2019), pp. 236-250

[14] X. Hu, K.G. Shin, S. Bhatkar, K. Griffin Mutantx-s: scalable malware clustering based on static features Presented as Part of the 2013 USENIX Annual Technical Conference (USENIX ATC 13), USENIX, San Jose, CA (2013), pp. 187-198

[15] Huang and Stokes, 2016 W. Huang, J.W. StokesMtnet: a multi- task neural network for dynamic malware classification Caballero J., Zurutuza U., Rodrguez R.J. (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment, Springer International Publishing, Cham (2016), pp. 399-418

[16] X. Zhang, J. Zhao, Y. LeCun Character-level convolutional networks for text classification Proceedings of the 28th International Conference on Neural Information Processing Systems, ume 1, MIT Press, Cambridge, MA, USA (2015), pp.

[17] D. Uppal, R. Sinha, V. Mehra, V. Jain - Malware detection and classification based on extraction of api sequences 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (Sep. 2014)

[18] A. Souri, R. Hosseini - A state-of-the-art survey of malware detection approaches using data mining techniques Human-centric Computing and Information Sciences, 8 (1) (Jan 2018),

[19] I E. Raff, J. Barker, J. Sylvester, R. Brandon, B. Catanzaro, C.K. Nicholas - Malware detection by eating a whole EXE - The Workshops of the the Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, Louisiana, USA, February 2- 7, 2018 (2018)

[20] A. Moser, C. Kruegel, E. Kirda - Limits of static analysis for malware detection Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007) (Dec 2007), pp. 421-43

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