



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

International Journal for Electronic Crime Investigation (IJECI)



VOLUME: 8
ISSUE: 3 Jul-Sep 2024

Email ID: ijeci@lgu.edu.pk

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

International Journal for Electronic Crime Investigation

Volume 8(3) Jul-Sep 2024

SCOPE OF THE JOURNAL

The International Journal for Crime Investigation IJECI is an innovative forum for researchers, scientists and engineers in all the domains of computer science, white Collar Crimes, Digital Forensics, Nano Forensics, Toxicology and related technology, Criminology, Criminal Justice and Criminal Behaviour Analysis. Moreover, the scope of the journal includes algorithm, high performance, Criminal Data Communication and Networks, pattern recognition, image processing, artificial intelligence, VHDL along with emerging domains like quantum computing, IoT, Hacking. The journal aims to provide an academic medium for emerging research trends in the general domain of crime investigation.

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.

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

International Journal for Electronic Crime Investigation

Volume 8(3) Jul-Sep 2024

CONTENTS

Editorial

Kaukab Jamal Zuberi

Modernizing Crime Detection: The Imperative of Technological
Integration in Pakistani Law Enforcement

01-02

Research Article

Zohaib Ahmad, Obaidullah, Muhammad Salman Pathan and Ahsan Wajahat
A Comparative Analysis of Malware Detection Methods Traditional
vs. Machine Learning

03-18

Research Article

Kausar Parveen and Kinza Batool

Advanced Techniques of Malware Evasion and Bypass in the Age of Antivirus

25-40

Research Article

Muhammad Asif Ibrahim, Syed Khuram Hassan and Maham Akhtar
Power of Homomorphic Encryption in Secure Data Processing

41- 51

Research Article

Ghulam Abbas, Ghulam Rasul Zahid

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth:
Challenges and Opportunities

52-66

Research Article

Zohaib Ahmad, Muhammad Ammar Ashraf

Enhanced Malware Detection Using Grey Wolf Optimization and Deep Belief Neural Networks

67-77

Research Article

Aftab Ahmad Malik, Waqar Azeem and Mujtaba Asad

Information Systems and Mechanism for Prevention of Cyber Frauds

78-88

Research Article

Rabia Mehmood and Zohaib

Live Memory Forensic: Capture and Analyzing Volatile Data

89-106

International Journal for Electronic Crime Investigation

Volume 8(3) Ju-Sep 2024

Patron in Chief: Maj General (R) Muhammad Khalil Dar, HI(M)
Vice Chancellor Lahore Garrison University

Advisory Board

Mr. Kaukab Jamal Zuberi, HOD Department of Criminology and Forensic Sciences, Lahore Garrison University, Lahore.
Dr. Abeo Timothy Apasiba, Temale Technical University, Central African Republic.
Dr. Atta-ur-Rahman. Imam Abdulrahman Bin Faisal University (IAU), Saudi Arabia.
Dr. Natash Ali Mian. Beaconhouse National University, Lahore.
Prof. Dr. M. Pervaiz Khurshid, Govt College Science, Lahore.
Dr. Nadeem Abbas, Linnaeus University, Sweden

Editorial Board

Mr. Kaukab Jamal Zuberi, HOD Department of Criminology and Forensic Sciences, Lahore Garrison University, Lahore.
Dr. Badria Sulaiman Alfurhood, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.
Dr. Muhammad Adnan Khan, Gachon University, Seongnam, Republic of Korea.
Dr. Faheem Khan, Gachon University, Seongnam, Republic of Korea.
Prof. Dr. Peter John, GC University, Lahore
Prof. Dr. Saqib Shehzad, Higher Education Department, Lahore
Dr. Shabbir Hussain, KFUEIT, Rahim Yar Khan.
Dr. Tahir Alyas, ORIC Director, Lahore Garrison University
Dr. Zahida Perveen, Lahore Garrison University.
Dr. Ahmed Naeem, Lahore Garrison University
Dr. Sumaira Mazhar, Lahore Garrison University.
Dr. Roheela Yasmeen, Lahore Garrison University.

Editor in Chief: Dr. Syeda Mona Hassan, Lahore Garrison University.

Associate Editor: Dr. Syed Ejaz Hussain, Lahore Garrison University.
Ms. Fatima, Lahore Garrison University.

Assistant Editors: Mr. Imran Khalid, Lahore Garrison University.
Mr. Qais Abaid, Lahore Garrison University.

Reviewers Committee:

Dr. Qaisar Abbas, Islamic University of Madinah, Madinah, Saudia Arabia.
Dr. Shehzad Ahmad. King Fahd University of Petroleum & Minerals, Saudia Arabia.
Dr. Haroon Ur Rasheed, University of Lahore.
Dr. Munawar Iqbal, University of Education, Lahore. Engr. Dr. Shahan Yamin Siddiqui. Minhaj University Lahore.
Dr. Saima Naz, University of Education, Lahore. Dr. Shagufta Saeed, UVAS, Lahore.
Dr. Shazia Saqib, University of Central Punjab, Lahore.
Dr. Mohsin Javed, UMT, Lahore.
Dr. Ayesha Atta, GC University, Lahore.
Dr. Nida Anwar, Virtual University of Pakistan, Pakistan.

Editorial

Leveraging Artificial Intelligence to Combat Electronic Crimes: The Case for Pakistan

Kaukab Jamal Zuberi

INTRODUCTION

In today's world, the importance of digital security cannot be overstated. Our reliance on electronic systems and internet-based transactions has created a vast digital ecosystem, but it has also paved the way for sophisticated cybercrimes. From financial fraud to corporate espionage and cyberterrorism, the range of electronic crimes is continually expanding, and so is the sophistication with which criminals operate. In many parts of the world, countries are countering these cyber threats by leveraging Artificial Intelligence (AI) as a core component of their cybersecurity strategies. Unfortunately, Pakistan lags in adopting these advanced measures, hampered by limited resources, underdeveloped infrastructure, and challenges in governance.

This editorial explores how AI is being used globally to combat electronic crimes, its potential benefits for Pakistan, and why there is an urgent need for Pakistan to bridge this technology gap.

AI and Cybersecurity: A Global Overview

In regions like North America, Europe, and East Asia, AI is increasingly central to cybersecurity, enhancing both proactive and reactive capabilities. Here are some of the ways AI has revolutionized cybersecurity globally:

1. **Threat Detection and Prevention:** Traditional cybersecurity solutions are rule-based and often detect only known threats. AI-driven systems, by contrast, use machine learning to identify unusual patterns and behaviors, detecting new and evolving threats in real time. For instance, unusual login patterns or unauthorized data access are flagged immediately, enabling rapid intervention.

2. **Predictive Analytics:** AI can analyze historical data to predict potential cyber-attacks before they occur. Companies like Darktrace and CrowdStrike use AI-driven models to assess vulnerabilities and enable proactive strengthening of security defenses.

3. **Automated Responses:** AI can automate responses to specific types of cyber threats. For example, if a network intrusion is detected, AI-driven systems can block IP addresses or isolate compromised areas without human intervention, saving valuable response time and minimizing damage.

4. **Fraud Detection:** Financial institutions worldwide rely on AI algorithms to monitor millions of transactions daily, identifying fraudulent transactions in real time by recognizing unusual spending patterns.

5. **Digital Forensics:** AI is also essential in digital forensics, enabling law enforcement agencies to quickly process vast amounts of data from

confiscated digital devices. This accelerates investigations, improves accuracy, and increases the chances of apprehending cybercriminals.

While these advancements are widely adopted in many parts of the world, Pakistan remains on the sidelines, relying on outdated cybersecurity measures that cannot keep up with the evolving nature of cyber threats.

The Alarming State of Cybersecurity in Pakistan

With rising internet penetration and a growing e-commerce sector, Pakistan has become a more attractive target for cybercriminals. Unfortunately, the country's existing cybersecurity measures are inadequate, creating an environment where cybercrime can proliferate. Key issues contributing to this weak cybersecurity landscape include:

1. **Limited Awareness and Education:** Cybersecurity literacy is low across Pakistan, affecting both the general public and professional circles. Poor awareness about online safety practices adds to Pakistan's vulnerabilities.
2. **Inadequate Legislation:** While Pakistan introduced the Prevention of Electronic Crimes Act (PECA) in 2016, it lacks the depth and enforcement necessary to counter sophisticated cybercrime. Moreover, enforcement remains weak, with law enforcement agencies facing shortages in specialized training and resources.
3. **Shortage of Skilled Cybersecurity Professionals:** Pakistan faces a significant shortage of trained cybersecurity professionals. The few

experts available are concentrated in the private sector, leaving government agencies and small businesses particularly vulnerable.

4. **Limited Investment in Technology:** In other countries, substantial investments in advanced technologies like AI are made to bolster cybersecurity. Pakistan, however, allocates limited financial resources to cybersecurity, with many public and private organizations hesitant to invest in AI-driven solutions.

5. **Weak Coordination Among Agencies:** Effective cybersecurity requires strong collaboration among government agencies, private companies, and international partners. In Pakistan, however, coordination is often lacking, leading to siloed efforts that cybercriminals exploit.

Why Pakistan Needs AI to Combat Cybercrime

Traditional cybersecurity methods such as firewalls, antivirus software, and manual surveillance are increasingly ineffective against sophisticated cyber threats. With criminals using AI tools themselves, Pakistan must adopt AI-driven cybersecurity solutions to:

1. **Enhance Threat Detection:** AI systems can identify and neutralize cyber threats faster and more accurately than traditional methods. Continuous monitoring and real-time data analysis enable the detection of suspicious activities that would otherwise go unnoticed.
2. **Improve Incident Response:** Cyberattacks can cause widespread damage within seconds. AI-driven response systems can automatically

execute defensive measures, significantly reducing response times and minimizing damage.

3. Streamline Digital Forensics: For law enforcement agencies, the ability to analyze vast quantities of data quickly is essential to tracking down cybercriminals. AI-based digital forensics can help agencies process data faster, speeding up investigations and improving prosecution rates.

4. Address the Shortage of Cybersecurity Experts: Pakistan's shortage of cybersecurity professionals is a major obstacle. AI can help by automating many tasks that would otherwise require human analysts, allowing the country to make the most of its limited cybersecurity workforce.

5. Bolster National Security: Cybersecurity is also a matter of national security, with cyber espionage, cyberterrorism, and other forms of cyber warfare on the rise. AI-powered solutions can help protect Pakistan's critical infrastructure, including government networks, power grids, and financial systems, from hostile attacks.

Barriers to AI Adoption in Pakistan's Cybersecurity

Despite the compelling case for AI in cybersecurity, Pakistan faces several challenges that hinder its adoption:

1. Lack of Infrastructure and Investment: AI-driven solutions require a strong digital infrastructure, including powerful servers and reliable data storage, which Pakistan currently lacks. The cost of establishing this infrastructure is also a significant barrier.

2. High Costs of AI Solutions: Implementing AI-based cybersecurity

measures can be expensive, especially for a developing country like Pakistan. Limited public and private budgets make the high initial costs of AI solutions prohibitive for many organizations.

3. Shortage of AI Talent: AI expertise is limited in Pakistan, with few educational institutions offering programs focused on AI and cybersecurity. To leverage AI effectively, Pakistan must invest in building a skilled workforce.

4. Privacy and Ethical Concerns: AI-driven cybersecurity often involves extensive data collection, raising concerns around privacy. Pakistan currently lacks robust data privacy laws, making it challenging to implement AI while protecting citizens' privacy rights.

5. Weak Institutional Support: AI adoption requires strong institutional backing, yet government support for AI-driven cybersecurity remains minimal, with few policies or incentives in place.

The Way Forward: A Strategic Approach to AI and Cybersecurity in Pakistan

For Pakistan to effectively combat cybercrime, a strategic approach that includes AI-driven solutions is essential. Here's how Pakistan can move forward:

1. Government-Industry Collaboration: Establishing public-private partnerships can help Pakistan leverage expertise and resources from its technology industry to advance cybersecurity capabilities. Joint efforts between the government and the private sector will strengthen the country's defenses.

2. **Investment in Education and Training:** Pakistan must invest in cybersecurity education, focusing on AI and related fields. Expanding specialized programs in universities will create a pipeline of skilled professionals to support cybersecurity efforts.

3. **Creation of a National Cybersecurity Agency:** Pakistan has previously attempted to establish a centralized cybersecurity agency to coordinate efforts across sectors. However, these efforts have temporarily failed, and cybercrime investigation responsibilities have reverted to the Federal Investigation Agency (FIA). For effective cybersecurity, Pakistan must renew efforts to establish a dedicated national agency that can lead AI-driven initiatives, promote public awareness, and foster international cooperation. This agency would also serve as a central authority for establishing and enforcing cybersecurity policies, addressing Pakistan's current fragmented approach.

4. **Incentives for Technology Adoption:** To ease the financial burden of adopting AI, the government could provide tax incentives, grants, or subsidies to companies investing in cybersecurity technologies. Encouraging AI adoption within the private sector is critical to building a robust cybersecurity framework.

5. **Strengthening Legal Frameworks:** Pakistan must update its cybersecurity laws, creating a regulatory framework that supports AI-driven solutions and addresses data privacy concerns. By establishing clear guidelines and penalties for cyber offenses, the

government can enhance deterrence and streamline enforcement.

Conclusion

As cyber threats evolve, the need for advanced cybersecurity measures becomes increasingly pressing. AI has emerged as a powerful tool for combating electronic crimes, providing capabilities beyond traditional methods. For Pakistan, the adoption of AI in cybersecurity is not just a technological upgrade but a necessity to secure its digital future. With renewed efforts to establish a dedicated cybersecurity agency, investment in education, and robust government-industry collaboration, Pakistan can begin closing the gap in its cyber defenses. By embracing AI-driven solutions, Pakistan can protect its critical infrastructure, strengthen its national security, and create a safer digital environment for its citizens.



Artificial Intelligence Based Techniques for Authenticity of Food Products in Food Fraud

Naureen Naeem¹, Bisma Naeem², Wasey Kareem² and Roha Naeem³

¹University of Agriculture Faisalabad

²Information Technology University Lahore

³National college of Arts. Lahore

Corresponding author: naureen.naeem@uvas.edu.pk.

Received: Jun 21, 2024; **Accepted:** Jul 27, 2024; **Published:** Sep 12, 2024

ABSTRACT

Food fraud is a widespread issue affecting almost all food commodities, leading to significant economic losses, public health risks, and violations of quality and consumer rights. Traditional detection methods are time-consuming, labor-intensive, and require costly equipment. With increasing competition in the food industry, there is a growing demand for faster, more efficient detection methods. Artificial intelligence (AI) and machine learning (ML) have emerged as powerful tools for predictive analysis in food fraud detection. These technologies allow for rapid analysis, aiding legal investigations ensuring food safety, authenticity, and traceability. Electronic nose (E-nose) systems, which identify organic compounds based on their unique aromas, are evaluated with chemometric methods to verify authenticity and help prevent fraudulent practices.

Keywords: Artificial intelligence; machine learning; food integrity; food safety; food quality.

1. INTRODUCTION

Food quality, food safety and food defense are part of the range within it falls "food fraud". The classification includes both

intended and unintended events true, whether the described result is actual harm to public health. The inspection and tracking

of foodstuffs through forensic techniques is categorized under the heading Food Forensics. While the global food supply chain is becoming increasingly complex and scalable, major changes in environmental as well as population-related aspects seem to have an influence on how our systems produce edible substances. But these changes could lead to more food fraud and safety issues, threatening public health. This is why we are beginning to see widespread use of artificial intelligence (AI) in the food supply chain as a serious method of mitigating these risks [1].

Other types of supply chain and traceability systems are also being considered for development to meet additional requirements surrounding food fraud. This surge of recent attention has food fraud now being pitched by commercial organizations as well as by governments in many countries. In the possibility of using forensic methods to authenticate and trace food products is included under an umbrella referred to as food forensics. From farm to fork, significant shifts in the environment, population and economy have an impact on how food producing systems will operate. These changes could result into higher risks related to food fraud which would also compromise safety and ultimately affect the health of people. One way to reduce these risks would be through applying artificial intelligence (AI) technologies within food supply chains. Artificial Intelligence is the ability of a machine to learn from big datasets statistically and then apply the results of this analysis to subsequent learning. The output produced as a result of this learning is algorithms, which are then used to meet specific needs. These needs are further improved because of autonomous learning, which is learning without human intervention. Machine Learning, as seen in the above definition related to Artificial Intelligence, involves giving structured

massive data plus continuous inputs on algorithms (way of improving them) and eventually train robots on how best they can respond. It's quite uncommon for a day to pass without hearing some headlines about how AI is going to revolutionize our lives. The potential uses are many because it can range from self-driving cars to sophisticated healthcare systems where machine learning algorithms help pathologists analyze tissue samples to generative AI that can produce text, images and audio. And it's all customized to what individual clients want. While the jury is still out on the benefits versus drawbacks of this technology, one area where AI/ML will greatly help humanity is in detecting food fraud and ensuring better food safety [2].

Food fraud is one of the major global challenges of our time, with AI/ML topping the list of technologies most applied in this sphere. Food fraud is an intentional act by food suppliers where products are misrepresented to the customer regarding composition, origin or quality. According to U.S. Food and Drug Administration stolen foodstuffs costs businesses between \$10 and \$15 billion annually. The cost to industry from yearly food fraud has been estimated at anywhere from \$10 billion to as high as \$40 billion with some figures going even higher than this range. Besides its financial implications, trust and safety in food because of fraud harmed customers. Fraud can take place in almost every field related with food sector and diverse varieties of foods including meat, fish & vegetable oils apart from beverages get impacted because of it [1].

Hardly does a day pass without some news feature reminding you about how AI will change the way we live our lives. Hardly a day passes without one of these news stories about the way AI is set to change our lives. The extent to which artificial intelligence (AI) and machine learning (ML) affect

humanity are constantly evolving. Generative AI: Text can be made germane to customer requirements when they need text, images when customers have image demands as well sound; infact the generative field seems limitless that could range from self-driving automobiles or taking machine learning on healthcare management perspectives like pathologists inputting tissue samples. One way AI and ML will help humanity is to improve food security by detecting food fraud. My sites that offer algorithms, convert large over time data sets to do statistical analysis learn through Artificial Intelligence [2].

AI (Artificial Intelligence) is the ability of a computer to analyze and learn through statistical analysis with large data. These things that these entities learn from is used other purposes, in the form of algorithms. An automated process, this continues unabated for as long as the algorithm is running and they get better with time. Structured big data sets and continuous algorithmic (product supervision) & human feedback with machine learning combines, AI systems can learn more precise. Food theft is the biggest global issue today and AI/ML is harshly being implemented on it. Simply put, food fraud is when a supplier gives inaccurate information to the consumer about what they are actually eating, an intentional act by any person or business for economic gain that misleads consumers as to what with product sold (composition, provenance and/or quality).

Aside from the financial implications, there is also a safety and consumer experience risk. Food fraud is a multibillion dollar industry, and food fraud incidents are rampant in nearly all common household staples like beverages, vegetable oils, fish, meat and poultry. A multiple consortium has always opposed food fraud in the food business. This includes assessments for raw material risk to identify high-risk supply

chains/materials. Analytical testing is conducted in response to these assessments to confirm non-negligible levels of adulterants that may be present in given foods [3].

These remain fruitful when the focus is on identifying adulterants, and fraud strategies have changed. However, the world of food fraud is a highly fluid one. Analytical chemists are always being fooled by criminals who add new adulterants, scam the tests and take advantage of this! This underscores the need for the non-aimed approach and establishes a sort of ongoing war between the scientists and scammers [4].

1.1. Leveraging AI

The ability of Artificial Intelligence (AI) to detect fraud cases which would have gone unnoticed with traditional approaches, is its capability of recognizing patterns in massive datasets. There are many online research articles and programs that work on chemistry and AI. One notable program is the United States National Institute of Standards and Technology's (NIST) "Machine Learning to Predict Food Provenance". The quality and the way consumers perceive food is heavily influenced by its origin in detecting food fraud. This is known as food provenance. Therefore, this is important to the economy as spoiled goods can be confused with much better commodities. At the 2019 NIST Food Safety Workshop, NIST identified one of the four main pillars of food safety as establishing computational tools and databases for determining food authenticity. They highlighted flaws in mathematical approaches to take on vast databases of biological and chemical information that would be necessary to define the fingerprint of food. The current focus of the NIST project to secure the American food supply

is the generation of chemometric fingerprints [2].

Food adulteration affects various types of goods e.g., Dairy, grains, and shellfish, oils and alcoholic drinks, honey. Even our fruits and vegetables are sometimes contaminated with toxic chemicals and pesticides. Adulteration almost always involves living essential things like food and water but can be made by removing key elements of a product, covering up lesser goods or substituting the real stuff with lesser products. Adulterants (Abuse) of food, food kept in harmful containers, and perverted pesticides or chemicals added to edibles, further damaging the quality. There are several factors in food potentially making it adulterated other than intentional adulteration, spoilage can also occur to fruits and vegetables or perishable goods such as dairy and drinks from microbial decay. The adulteration and contamination of food are serious health hazards that can cause inferior quality [5].

Initially such worries were trivial but with the social and economic upliftment of society there is a growing concern over safety and standardization of food. As more and more people are becoming aware of the benefits of living healthy a good food pollution detection serves the primary objective for which it is needed. Currently, the rapid increase in the international turnover of food has been accompanied by a rising demand for high-quality food. Nonetheless, traditional food analysis methods are often limited as they rely heavily on subjective quality assessment [3, 4, 5].

In this context, biosensors and artificial intelligence (AI) bring new approaches for food quality evaluation. Thus, this study puts forward a detailed work on designing evaluation models suitable for any level of aggregation for data which will in turn be combined with food quality indices. This is

to demonstrate the precision and effectiveness of AI and bio-sensors for food quality testing. The use of AI and ML for food fraud detection has been well researched. When the rice's origin was asked about or premium-quality rice had been mixed with low-quality rice, there were some cases in which fake rice samples were distinguished using E-nose sensors and near-infrared spectroscopy. In another study, a machine-learning model was developed and applied to Fourier-transform infrared spectroscopy data from milk adulterated with eighteen different substances (from melamine to water) [6].

Another study conducted hyperspectral sensing and RGB imaging data with AI/ML to detect artificial ripening of bananas using expression of calcium carbide, which is carcinogenic in ethylene based ripening. All these as well as many other examples show how AI and ML are being used to perform an untargeted manner of this approach may surprise older generation of analytical chemists. Traditionally, identifying an adulterant meant first figuring out what the adulterant was and then devising an analytical technique to screen for it. For years, this targeted approach was the main strategy. Computer evolution allows the effective analysis of vast data collections employing data never done before. The data scientist of today reviews the data available and tells if a sample is skewed, hence tampered with or not. It is now good enough to determine whether the material is identical or not; it no longer has to be this same Molecule you wanted. AI and ML shines in this type of non-targeted approach. It can be from any of the data sets to analyze [7].

Artificial intelligence used in identifying food fraud can be greatly enhanced with the establishment of new cutting-edge chemical databases and their widespread publication. To solve this problem, this enclosed world

of food firms will eventually need to open up and share data with one another in order to develop important algorithms that can be used for creating a safe and reliable food chain [8].

Food adulteration is a dangerous and morally corruptive practice that contravenes the most elementary rules of food science and puts public health at risk. It is the act of surreptitiously substituting harmful elements in substandard goods with a high margin for profit. He said the unethical practice has evolved into a billion-dollar industry, with shopkeepers, vendors and others seeking to turn fast profits at the expense of health safety requirements. Dairy, grains, shellfish, oils, alcoholic beverages and honey are just a few of the many products affected by food adulteration. Pesticides and other hazardous chemicals ruin even the fruits and vegetables. Adulteration is the use of dishonest methods or impurities in food and drugs with the intent to deceive consumers; for instance, removing vital ingredients from food hiding low-quality goods or selling one thing as another. Along with the unclear components going in, food is also stored in hazardous containers, and there are dangerous chemicals or pesticides that come along. In addition, food contamination can occur spontaneously with the deterioration of perishable items such as dairy and liquids or when microorganisms spoil fruit and vegetables. Due to adulteration and contamination, it becomes an important issue that affects the health of the consumer [6].

As such, food safety and quality are increasingly of concern as society develops socioeconomically. As awareness grows about the importance of healthy eating, so does the need for a food pollution detector. Meanwhile-thanks to the incredible pace of global food trade as well the need for better quality food has become even more

pressing. The vast subjective nature of traditional food analysis methods to underpin the quality assessment and, therefore, often with their limits. Therefore, the development of biosensors and artificial intelligence (AI) enable new strategies of food quality assessment. This work provides an extensive methodology, which deals with evaluation models consistent to the food quality indices and their associated information. This aims to showcase the broad scope and effectiveness of AI and biosensors in analyzing food quality. This study also addresses the difficulties and opportunities that these technologies may present [9].

1.2. Transformative potential of AI and ML in detecting Food Integrity

The integrity of food is a complex and multi-dimensional problem. Conventional ways of monitoring food quality and safety are manual inspection testing, which is time-consuming and even prone to errors made by human. A solid monitoring process is needed to address these concerns and to catch misappropriation of quality in food, before it becomes a common thread at a source. Such technologies, which is why AI and ML are blossoming as a silver lining and new conquest. Tied to the aforementioned benefits, these technologies have the capacity of resolving intricate issues and producing novel solutions with practical use cases, notably in strengthening food safety and quality monitoring systems by making them more accurate, quicker and efficient as well. But the issue of food integrity is much more complex, and traditional methods for safeguarding food safety and quality rely on time-consuming, manual testing or observation susceptible to human error. To respond to these challenges, food companies must deploy robust track-and-trace solutions capable of spotting problems with

food quality as early in the production process as possible. Artificial intelligence (AI) and Machine Learning (ML) technologies are indeed a relatively newer space that is beginning to provide potential solutions to these critical issues faced by the food chain. Beyond gaming, AI and ML are

proven to handle hard-to-tackle problems, as demonstrated by recent publications that have proposed innovative solutions to address practical issues related to enhancing the precision, efficacy, and efficiency of food-safety or -quality monitoring systems [10].

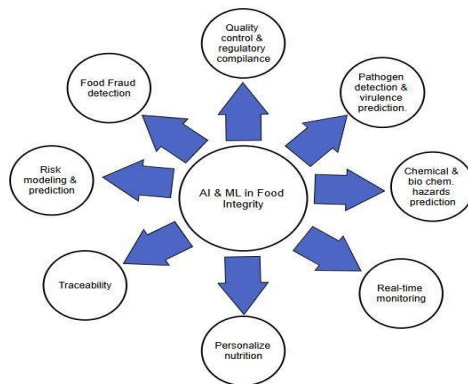


Figure 1: Applications of AI and ML in Food Integrity

By using AI and ML technologies, the automated systems can establish accurate and uniform quality parameters for different types of food products based on changes in shape, size, color, texture, and nutraceutical composition; they maintain product quality during processing. By processing large food safety datasets such as those of Food Safety Modernization Act (FSMA), the predictive AI/ML models can forecast future occurrences, identify attention deficient areas and aid in develop useful food safety management plans. The information helps food safety people make decisions ensuring a safe food supply, and to develop interventions that can be more responsive with resources [10, 11].

A study for instance that enhanced the border inspection of imported food to Taiwan developed a range of ensemble learning models anticipates food security risks. These models were used online, and it will be a long non-conformity hit rate with that, which shows how nicely ensemble learning works to give us signals of where the food safety hazards are going into. Alternatively, Support Vector Machines (SVM) were using to devise an intelligent early warning system for the detection of food safety threats and their possible outcrops [12].

The distribution of records on food, health, and agriculture across multiple domains and many not in digitalized formats raises a challenge for food safety. By merging data

from numerous places and transforming those documents into a computable format, modeling can become quite effective. Combining data from different sources together can provide a more complete picture of the attributes and factors that influence food safety outcomes e.g. mycotoxins, toxic compounds produced by some fungi, depend on temperature and humidity. Incorporating climatic data into modeling contexts allows for an appraisal of which environmental factors influence mycotoxin levels in food products [13]. This richer data source expands the types of inputs that can be used to build models, allowing for larger quantities of related (or even weakly related) data to be factored into model creation thereby uncovering more intricate relationships and patterns between varying prismatic product elements that might not otherwise become clear in a significantly smaller set. In this broader sense, we can learn more accurately and in a nuanced way about what affects food security, resulting in stronger, more capable models. At present, AI and ML technologies are now capable of grade quality attributes of different food staples as shape, size, color, texture etc. and help to keep them in good condition while they undergo processing under automated systems [14]. Predictive AI and ML models can accurately predict the probability of future occurrences, identify hot spot areas and can enable greater data analytics from large food safety datasets for designing effective food safety management systems. Food safety experts can leverage this information to help them design more resource-efficient treatments so as to maintain quality and integrity. The study [15] analyzed the prediction for food safety risks across many ensemble learning models but mainly prioritizing measures to enhance border

inspection of imported food into Taiwan. This improved the hit rate of non-conformities drastically with the implementation of their online approach models; this is a good example of Ensemble Learning for forecasting the risks related to food safety. An intelligent early warning system for food safety issues was developed utilizing SVM for prediction of potential alerts related to food safety other than conventional QSAR processes for more secure food supply chain [14, 15, 16]. Another area of concern is the pervasive anonymity of numerous food safety records, which still exist in non-digitized format and are dispersed across various sectors (such as food, health, agriculture). These papers were then combined digitally so it would be computationally friendly, and additional information was added from numerous sources which allow for the creation of large datasets to enhance its efficiency and capability. By aggregating data from multiple sources, one is better able to capture a broader set of characteristics and covariates that contribute to the outcomes of food safety Test Category. This integrated view leads to a more comprehensive understanding of the complex interconnected relationships and dynamics in food safety. Mycotoxins, here represented by toxic compounds produced by certain types of molds, are a good example which can be altered or catalyzed by environmental agents such as temperature and humidity. The climate data can then be incorporated in the form of covariates into the modeling and provide insights to know about the environmental factors that drive higher or lower mycotoxin levels in food products. The higher number of data allows revealing subtle connections and clues which become invisible if you use a small volume, moreover there is more material for

modeling. This enables to more accurately (as well as more complexly) describe the multiplicity of factors that can influence food safety, leading eventually to models that generalize much better [17].

1.3. Role of AI and ML Techniques in Food Safety and Quality Control Assessment

AI and ML techniques have transformed the field of food quality management by providing innovative methods for enhancing the consistency and safety of food products [18]. A few most common methods used by the industry are:

1.3.1. Computer vision

AI and machine vision have literally been a landmark solution in food process engineering [19]. And this duo is paving the way for a transform in the industry of food, whereof allows thorough and automated visual inspections. Food testing through image and video analysis is precisely and quickly examined by AI-powered computer vision systems. Those systems are critical for things like sorting, grading and evaluating quality. By detecting deviations from quality standards in time, they ensure that only the goods complying with these stringent requirements are delivered to consumers. This has effects on numerous food processing segments. During Sorting, AI can identify very fine variation in color, size, and form during the process of sorting by using computer vision system. This ability to very finely group makes product identification straightforward and it is particularly useful where uniform good quality of fruit/vegetable grading / sorting products is needed.

In addition, computer vision gets rid of food safety concerns by quickly spotting pollutants or pathogens. It allows organizations to respond quickly, which, in turn, minimizes food safety vulnerabilities or threats and avoids recalls. They provide objective scores over the consistent aspects of qualities defining customer preferences within quality evaluation. They make product evaluation standard as far as possible by reducing human subjectivity that in turn fulfills customer satisfaction and confidence. Shorter Procedures AI and computer vision combine to improve resource use/resource planning. By detecting defects earlier thereby reducing waste, which reduces costs and increases sustainability.

1.3.2. Sensors and spectroscopy

Research stated that machine learning (ML) algorithms assess key properties moisture, pH values and chemical structure by examining data from diverse sensors as well as spectroscopic methods. Given AI's knack for gauging nutritional value, ripeness and freshness estimation, producers might be in a better position to optimize production and storage methods based on this data-driven analysis. Safety assessment and quality control the analysis of sensor data or spectroscopy that AIs can do typically far exceeds that of what a human can handle.

AI enables producers to identify patterns and thus minimise resource wastage or maximise their manufacturing efficiency. Also, Real-time sensor data streams align with contemporary paradigms such as Industry 4.0 and The Internet of Things (IoT) which allows to predict quality deviations and take appropriate actions in a timelier manner. This hybrid AI and ML in conjunction with spectroscopy and sensors

is an incredibly powerful yet underused magic wand which can not only improve the efficiency of operations in food manufacturing but also protect the foundation of food safety and quality laying into ever-changing complexities of the dynamic field of food process engineering [20].

1.3.3. Predictive modeling

AI and ML interactions in the predictive modeling are of great concern to quality assurance over precise notions of food quality. Si et al discussed this approach in detail, which derives plausible anomalies through training a ML model on historical data and also estimating the perishable shelf-life of food items as part of forecasting quality issues [21]. AI and ML enable easy monitoring of various parameters during production and storage. This allows the system to make an estimate on when contamination, spoilage or other forms of decay will happen. Producers can make faster and informed decisions with such AI-powered predictive models, as it helps to discover patterns and connections in the data. As a result, immediate response can be given to protect end product integrity, minimize waste and ensure that food producers market high quality and safe products to customers. In other words, using predictive modeling enhanced by AI could provide a big jump in the food process engineering field. This strategy improves the industry's capacity to reduce risks, maximize resources, and eventually provide goods that satisfy the highest standards of quality and safety by utilizing historical insights and real-time data.

1.3.4. IoT-enabled real-time monitoring

Another research reported AI and ML integration had led to the development of a variety of IoT devices with built-in sensors. It is also possible to monitor vital metrics in real time thanks to this collaboration which makes quality control proactive. This new breed of BI (Business Intelligence) technologies can capture the data in real time with these IoT devices, ensuring that the quality standards are always met. AI systems check data when deviations detected send out notifications quickly alerting when you need to take action fast. This entire process allows for minimal intervention, potentially preventing errors and cross-contamination, creating faster reaction times.

Quality control processes can be facilitated by means of robotics and automation propelled by AI as well. By eliminating human involvement, these technologies make the chances of errors drop to almost nil and hence offer precision. So, that Food products can easily be examined, and handled more consistently so the quality is there, with no unnecessary wastages. In short Utilizing AI, ML and IoT with Food Process Engineering make the industry even more bolstered to maintain its quality. Trust, satisfaction and general efficacy are raised by the application of real-time monitoring and automatic reactivity which ensure stakeholders that only top-notch products are delivered to the customer [21].

1.3.5. Data-driven decision making

Si et al. [22] a recent perspective and forecast paper in the area of food process engineering have brought AI and ML at a similar pace toward convergence using extensive data (big data) for high-throughput decision-making. This approach involves the aggregation of multiple

datasets like manufacturing logs, customer feedback or lab results. Since the solution is capable of analyzing and processing immense datasets, it opened doors to AI-powered improved quality control systems. This combination also makes it easier to find complex patterns and issues which can be missed using traditional methods. Artificial Intelligence (AI) to improve SAS quality assessment accuracy through identifying trends and abnormalities across a number of dimensions. It also allows you to identify potential problems proactively. An applaudable step toward data-driven decision-making is the advent of AI and ML in food process engineering. This clearly not only promotes industry involvement and improvement but also enforces meaningful consumer perception of product quality.

1.3.6. Greater transparency and traceability

The fusion of AI and block chain has proven beneficial in notably improving transparency as well as traceability throughout the food value chain. Recently, in a study tracing food from where it is produced to its final consumption point using these new technologies was highlighted and found to be very beneficial. The use of AI-powered block chain data analysis allows targeted and immediate source identification in cases of contamination or recalls. This provides more leverage on corrective actions and enhances consumer safety as well as underscores the need for efficiency in traceability systems. More than extraordinary data clarity to supply chain keeping actors, this convergence of block chain and AI along with food process engineering also asserts for the moral pillar and responsibility. These solutions offer a

new generation of food safety and quality assurance that innovation will propel by fostering transparency for higher industry standards to ensure customer trust [22].

1.3.7. The connection of AI and ML

Techniques are a game changer that caused important transformation in the management area, mainly food quality control as this will help us to be more customer centric and have lesser coming back with dissatisfaction giving less waste and more power in safety. Even in the developed world, there is open space for further improvement in quality of food control systems that would assure a constant supply of safe and good food products. These technologies have made the food process engineering field very different from what it was before in a sense of how much more efficient, accurate and reliable it has become. This is a very relevant key testimony for the direction of quality assurance in food, as its outcomes reveal a cooperative synergy between food science and AI and ML [20, 21, 22].

2. Enhancement of Food Safety and Quality Control by Sensor based AI and ML

AI-based sensing technologies have successfully applied to collect and analyze data by utilizing the AI algorithms built on sensor data, which enables the extraction of useful information. For various domains ranging from environmental monitoring, healthcare to agriculture and so forth we are using modern sensing technologies. Fig. [1] depicts application of AI and ML in the food business Artificial Intelligence (AI)-enabled sensing technologies have emerged as the next frontier in managing food qualities

across their supply chain while maintaining safety and integrity [23, 24, 25].

2.1. Food Manufacturing, Processing, and Storage IoT-enabled smart sensors

The IoT devices and intelligent sensors are changing the way the food is produced, processed and stored. The sensors can monitor chemical compositions, pH levels temperature, and humidity, as well as gas emissions. The intelligence gained from these sensors, in real time, can provide notifications on the quality and safety. By joining together, we can take the monitoring system to the next level of dynamicity that provides better possibility in food manufacturing by maintaining ideal conditions while avoiding the creation of microorganisms and other bad impacts caused by moisture. Furthermore, it ensures safety by detecting unusual gas emissions and following chemical compositions, allowing prompt involvements and preemptive actions [26].

2.1.1. Sensors for image and spectroscopy

In contrast, others studies described AI-driven images in addition to the acquired spectroscopy sensors that can transmit information on some chemical and sensory state of food products. Computer vision algorithms driven by artificial intelligence (AI) can inspect images much more thoroughly than the human eye, for both defects and anything inside food. It then benefits the quality control process in food manufacturing. Moreover, by capturing the phenomenon of food and light interaction in detail, spectroscopic sensors have a crucial role to play in understanding what lies beneath with regard to nutrition and composition as well as freshness of food. That's where this AI enable in an advance analysis which leads to more

accurate and faster to determine food quality. [23] [24] [25].

2.1.2. AI based gas and odour sensors

A study demonstrated the significance of AI-enabled gas detection for food production and safety highlighted twelve dangerous substances, spoilage and malodorous compounds that are released from food materials [25]. These sensors are able to utilize the capacities of AI and interpret sensor data quickly and accurately. So products that do not meet the standards or wear out very quickly, ensuring they will be push out of the production line before buyers purchase them. Besides this, reducing potential well-being risks, this active strategy guards the integrity of the food supply chain overall and the producers' reputation. The consequences provide a strong illustration of how merging AI and sensor technology develops food safety methods ensuing raised quality assurance and higher consumer confidence.

2.1.3. Nanosensors

A study looked at the changing game around food safety and processing in relation to nanotechnology namely nanosensors. As it allows the identification of substances and diseases on a molecular level, AI-nanosensors are indispensable for determining food safety with the newest technology. Thus, these nanosensors enable a quick and accurate detection of contaminants in essential consumables. With the help of nanosensors, which can pack the power of AI woodchip processors to secure automated food safety practices. The fusion of artificial intelligence with nanotechnology in food safety scenarios is a revolutionary breakthrough. Not only this

ushers in a new era of precision and reliability in the food supply but also enhance the monitoring and controlling of contaminants. Manufacturers can, therefore, strictly follow safety regulations and consumers are more confident about the products that they use [26, 27].

2.1.4. Integration of Blockchain

In another study, integration of blockchain technology with AI sensing was referred to as potential disruptive technology and found solution to enhance food processing and safety that records immutable ledger across the entire supply chain of the food, increasing data security and track-ability, this win-win cooperation. When the data is from sensors, it is recorded with block chain technology to guarantee transparent and durable. This seamless integration of capabilities ensures compliance with stringent QA norms, facilitates a risk reduction and enhances operational efficiency. One major evolution is the integration of blockchain with artificial

intelligence (AI). This fosters accountability, enables transparency in sourcing and tracking real-time information by the stakeholders as well as builds customer confidence in food items.

2.1.5. Remote sensing

Studies shows the authors consider AI-powered methods that could be employed to enhance sustainability of food safety and processing. Drone and satellite-based technologies help the quality of food stay up to par by evaluating crop vitality and environmental factors identifying abnormalities, such as pest infestations and temperature swings. Remote sensing using AI gives real time results, which helps in decision-making and quick actions to avoid some sort of disasters. Responsible for supporting all Food Safety & Quality Control systems and abiding by the requisite regulatory requirements to ensure the integrity of food production in accordance with Food Safety Guidelines. [25] [26].

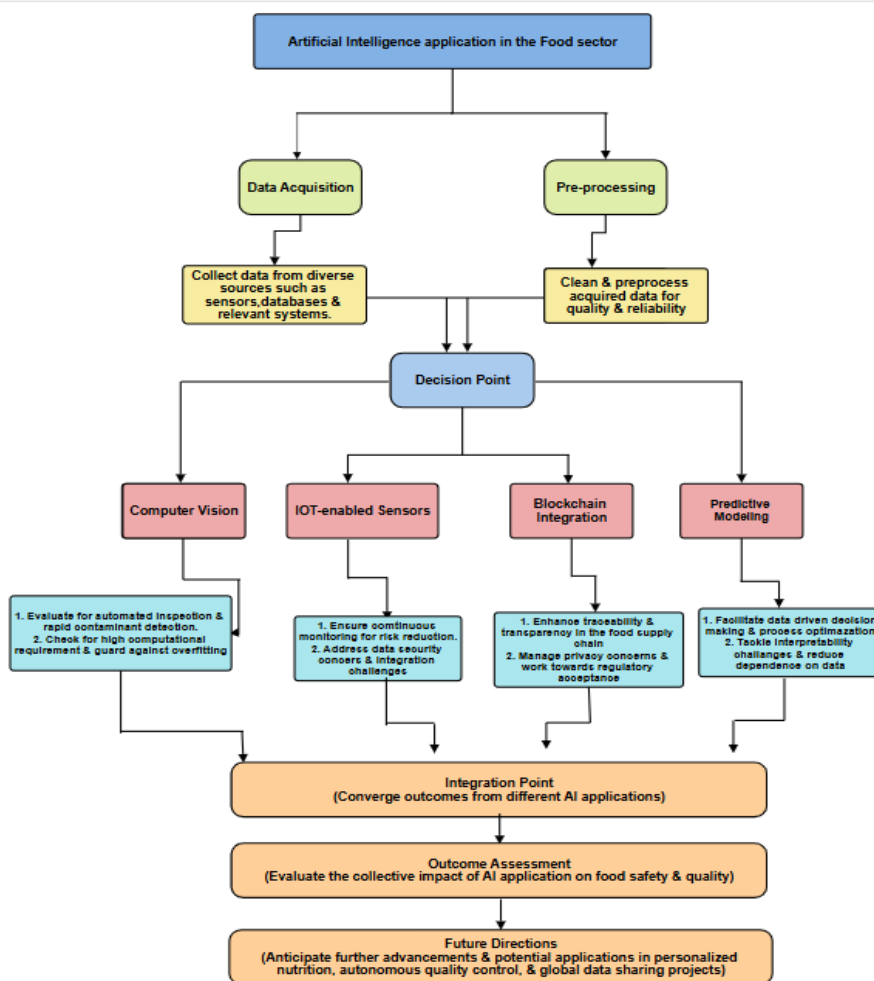


Figure. 2: Flow chart showing an important role of artificial intelligence in food sector [12]

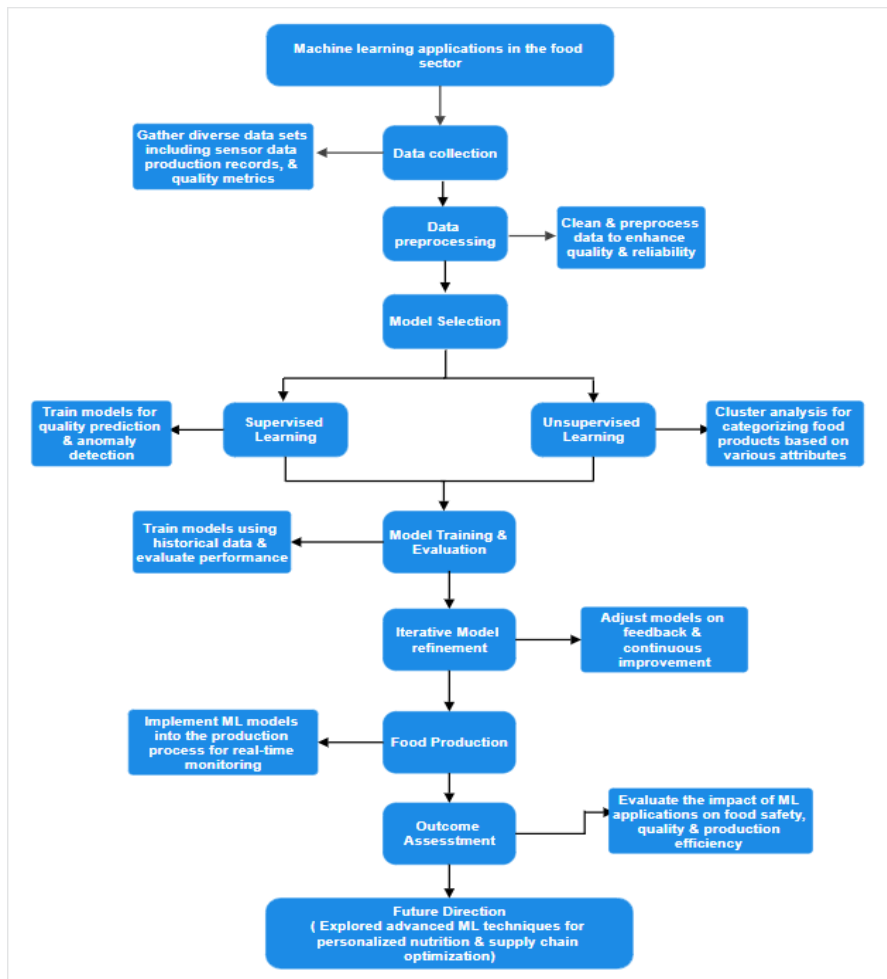


Figure 3: Flow chart showing a crucial role of machine learning in food sector [12]








3. Overview of AI techniques used in food quality and adulteration

Computer systems capable of doing human like tasks are generally called Artificial

Intelligence (AI). Machine learning and deep learning, for instance, typically used in the intricate systems for modeling, control, optimization identification prediction

estimation and more. Summary of AI techniques applied to food and beverages

adulteration and defect detection in fruits illustrated in Fig 4.

AI TECHNIQUES			
BEVERAGES Black Tea Milk	FOODS  Olive Oil Sesame Oil	¹ ANN	FRUITS Peaches Cucumber
BEVERAGES  Milk Powder Coffee	FOODS Rice Mutton Wheat Flour Peanut Honey Extra Virgin olive oil Avocado oil Edible oil 	³ CNN	FRUITS Pineapple Apple Oranges Pear Mangosteen Dates Citrus/Lemon Potatoes Tomatoes Cucumber Strawberry Blueberry Mulberry Sugar Beet fruit
BEVERAGES Milk	FOODS Sea cucumber Minced meat Beef Casava starch Saffron Ginseng Butter oil Sesame oil Honey 	² SVM	FRUITS  Blueberry Chilli Peppers Peaches
	FOODS Ground nutmeg Cream	⁴ RF	FRUITS  Strawberry Apple
	FOODS Beef	⁵ FL	FRUITS Olive Pineapple 

¹Artificial neural network (ANN), ²Support vector machine (SVM), ³Convolutional Neural Network (CNN), ⁴Random Forest (RF), ⁵Federated learning (FL)

Figure 4. Overview of AI techniques used in food and beverages adulteration and fruit defect detection.

This demands a collaborative approach so that all the players of food supply chain are identified, verified and certified; bad ones get ousted; and food is traced back in real time. The review discusses numerous technologies currently found in the market to detect food adulteration and multicultural pattern recognition tools. This article provides some context about the forces behind food fraud, such as economically

motivated adulteration, from both the perspectives of industry and consumers. Key points in this issue are policies for the integrity of food chains. In future, it can even be useful for academics to consider the approach these challenges more interdisciplinary and concentrate in areas such as food adulterers, food security and climate change.

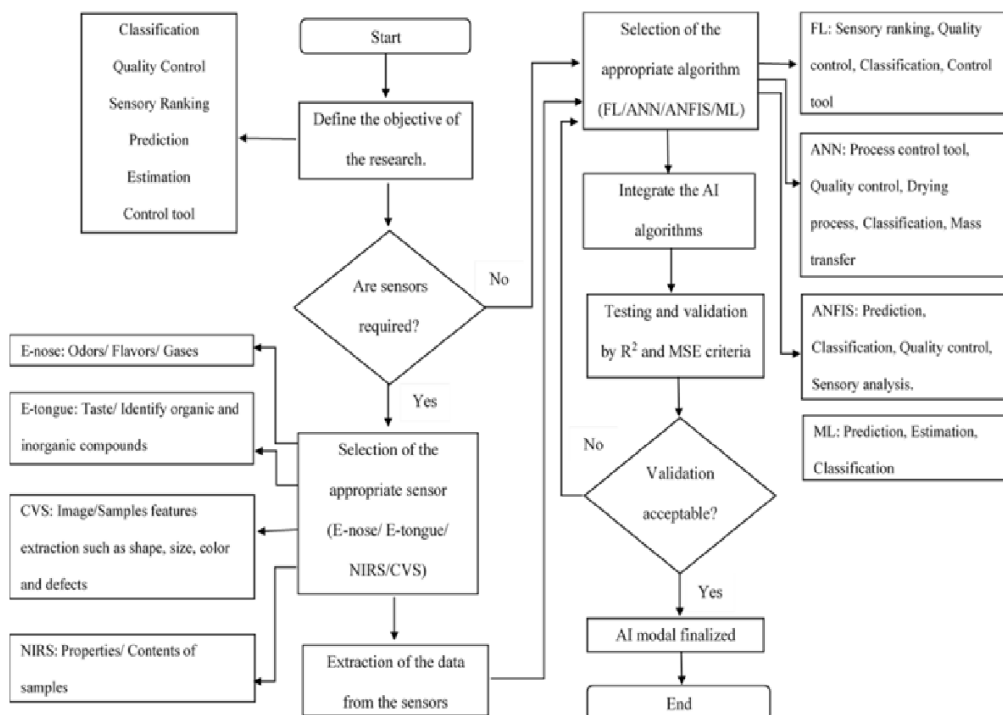


Figure 5. Flowchart for developing AI model in Food Processing

4. Use of E-Nose and E-Tongue for Food Authentications

E-nose and E-tongue, employed to mimic the capability to smell and taste perceived by human beings, provide an In-situ, rapid, reliable, and objective way of assessing food samples and mitigating increasing concerns regarding food integrity. Thus, integrating electronic sensors with chemometrics and pattern recognition methods appears to be an effective approach for food authenticity study.

Introduction Analysis of food supplies is now performed with the help of powerful analytical instruments known as E-nose and E-tongue. Possible future applications of E-nose and E-tongue to food authentication are promising. Hence, advances in sensor technology combined with developments in data analytics and ML will bring new possibilities to the next level of food quality control and consumer protection. Besides representing massive real-world uses in the area of food validity, a number of policies can be used to upsurge their

critical efficacy. It has been presented that food safety is ensured by integrating E-nose and E-tongue technology into altered phases of the food supply chain [23, 24, 25, 26].

5. Food Fraud Investigation with special context to Pakistan

A number of food Authorities are now working at both federal and provincial level in Pakistan. In particular, the Punjab Food Authority (PFA). Founded in 2011, it has been engaged in improving the food safety and quality of Punjab. It checks, runs the sampling and testing of the food campaigns and is responsible to set food safety and hygiene quality standards only to make aware about food safety among public and manufacturers and also guide the same for ethical safe and hygiene food process, assure compliance as per established guidelines /Standards. The first specific food safety legislation at the national level was enacted with the West Pakistan Pure Food Ordinance of 1960 and cantonment Pure Food Act of 1966. The basis of these laws ensured that foods were safe at every level from production to the consumption. There are also various regulatory bodies such as the Pakistan Standards and Quality Control Authority, which is tasked to regulate food safety in general. They offer consultancy, testing, certification services and control quality specifications and monitoring. Consumers: Consumers are critical to safe food production and accurate labeling [26].

6. Conclusion

In recent years, the global food supply has become more complex and dynamic. The functioning of the food industry from farm to fork is affected by the changes in the environment, population, and economy. These changes will increase the number of food frauds and insecurities that will harm people's health. The use of artificial intelligence (AI) in the food industry is one strategy to reduce these dangers. The use of AI has increased in many sectors such as food safety, automotive, precision agriculture, precision medicine, and food security. This study has several implications for practitioners and researchers. It is believed that research on artificial intelligence (XAI) can help bridge the gap between machine learning models and human decision-making in food safety. In addition, consumers, regulators, and other stakeholders can better understand how to predict and manage food safety with the help of educational models. For scientists, more accurate models can be created by analyzing existing models interpreting their predictions, because with the help of the XAI model, the advantages and disadvantages of the model can be seen. This article provides a practical review of food justice imaging, particularly AI and machine learning, and outlines current advances and trends in this area. Key areas of focus include the use of AI and machine learning in quality control and monitoring, food fraud detection, process control, risk monitoring, prediction and management, and chain traceability. The use of AI and machine learning in the food industry has improved health standards, thereby

improving consumer health and confidence, and making food more energy efficient. While these applications hold great promise, this article also acknowledged some of the challenges in using these capabilities in certain areas of the food industry. This article highlighted the prospects and trends, and emphasized the importance of overcoming these challenges to achieve the potential of AI and machine learning. The food industry faces challenges such as changing consumer behavior, competition, food safety risks, and the responsibility of those working in the industry to adhere to strict safety standards, ensuring the integrity of food and the quality of the production process. In this review, general approaches toward research and development of AI and machine learning in food fraud detection is examined including food research, quality control, chain traceability and transparency in risk assessment and hazard prediction, health point monitoring, foodborne illness detection, and prediction. The document concludes with a call to action to continue research, innovation and collaboration, highlighting the incredible promise of combining AI and machine learning with technology to create a safe and sustainable global food supply.

REFERENCES

- [1] Y. Ye, D. Wang, T. Li, D. Ye and Q. Jiang, "An intelligent PE-malware detection system based on association mining", *Journal in computer virology*, vol. 4, pp. 323-334, 2008.
- [2] A. Aimi, G. Viejo, C. P. Alexis and F. Sigfredo. "Rapid Detection of Fraudulent Rice Using Low-Cost Digital Sensing Devices and Machine Learning", *Sensors*, vol. 22, no. 22, pp. 24-41, 2022.
- [3] G. Sefater, N. Patrick, "Enhancing Food Integrity through Artificial Intelligence and Machine Learning: A Comprehensive Review", *Applications of Science*. vol.14, no. 8, pp. 3421-3435. 2024.
- [4] E. M. Alotaibi, "Risk assessment using Predictive Analytics". *International Journal of Professional Bussiness Review*, vol. 8, no. 5, pp. 01-25, 2023.
- [5] W. L. Ya and W. S. Shun. "Ensemble Learning Models for Food Safety Risk Prediction". *Sustainability*, vol. 13, no. 21, pp. 01-26, 2021.
- [6] Z. Yu. "Food Safety Risk Intelligence Early Warning Based on Support Vector Machine", *Journal of Intelligent Fuzzy System*, vol. 8, no. 38, pp. 6957-6969, 2020.
- [7] W. Xinxin, B. Yamine, L. A. O. Lansink, V. F. Klerx, "Application of Machine Learning to the Monitoring and Prediction of Food Safety: A Review", *Comprehensive Reviews in Food Sciences and Food Safety*, Vol. 21, no. 1, pp. 416-434, 2022.
- [8] W. Saak, G. Lan, V. Car, B. M. Jeroen. "Big data in smart farming: a review", *Agriculture*

- Systems*, vol. 153, pp. 69-80, 2017.
- [9] K. Vijay, N. V. Huan, K. B. Parveen, K. Hakil and P. V. Rao. "A critical review on computer vision and artificial intelligence in food industry", *Journal of Agriculture and Food Research*. Vol. 2, pp. 1-12, 2020.
- [10] B. Brandon, M. Guillermo and M. Sarah. "Scaling up agricultural research with artificial intelligence", *IT Professional*. vol. 22, no. 3, pp. 33-38. 2020.
- [11] S. Konstantina, K. Erisa, S. Uthayasankar, D. Stella and I. Zahir, "Artificial intelligence and food security: swarm intelligence of agritech drones for smart agrifood operations", *Production planning and Control*. vol. 33, no. 16, pp. 1-19. 2021.
- [12] S. Othman, N. R. Mavani, M. A. Hussain, N. A. Rahman and J. M. Ali. "Artificial intelligence-based techniques for adulteration and defect detection in food and agricultural industry: A review", *Journal of Agriculture and Food Research*. vol. 12, no. 4, pp 1-16, 2023.
- [13] D. R. Mavani, J. M. Ali, S. Othman, M. A. Hussain, H. Hashim, N. A. Rahman", Application of Artificial Intelligence in Food Industry a Guideline", *Food Engineering Reviews*, vol.14, pp134-175, 2022.
- [14] R. Bernadette, R. Marc, G. Stephanie, K. Oliver and F. Markus. "Food monitoring: screening of the geographical origin of white asparagus using FT-NIR and machine learning", *Food Control*. vol. 104, no. 29, pp. 318-325, 2019.
- [15] C. Qian, S. I. Murphy, R. H. Orsi and M. Wiedmann. "How Can AI Help Improve Food Safety?" *Annual Review of Food Science and Technology*, vol. 10, no. 4, pp. 517-538, 2023.
- [16] B. Yamin and M. Hanz. "Prediction of Food Fraud Type using data from rapid alert system for Food and Feed (RASFF) and Bayesian Network Modelling", *Food Control*, vol. 61, pp. 180-187, 2016.
- [17] B. S. Mithun, S. Shinde, K. Bhavsar, A. Chowdhury, S. Mukhopadhyay, K. Gupta, B. Bhowmick and S. Kimbahune. "Non- Destructive Method to Detect Artificially Ripened Banana Using Hyperspectral Sensing and RGB Imaging", *Proceedings of the Sensing for Agriculture and Food Quality and Safety X*, Orlando, FL, USA, 10665. pp. 122-130. 2018.
- [18] P. K. Kumar, K. V. Naveen. "Qualitative and Quantitative Detection of Food Adulteration Using a Smart E-Nose", *Sensors*. vol. 22, no. 20, pp 1-16, 2022.
- [19] F. B. Santana, W. B. Neto and R. J. Poppi. "Random Forest as One-Class Classifier and Infrared Spectroscopy for Food Adulteration Detection", *Food Chemistry*, vol. 293, pp. 323-332, 2019.
- [20] K. Lim, K. Pan, Z. Yu and R. H. Xiao, "Pattern Recognition Based on Machine Learning Identifies Oil Adulteration and

- Edible Oil Mixtures”, *National Communications*, vol. 11, no. 1, pp 1-11, 2020.
- [21] Y. Si, G. Liu, J. Lin and F. Juan, “Design of control system of laser levelling machine based on fussy control theory” *International Conference on Computer and Computing Technologies in Agriculture. Springer*, Wuyishan, China, pp. 1121-1127. 2007.
- [22] S. A. Laga and R. Sarno, "Temperature Effect of Electronic Nose Sampling for Classifying Mixture of Beef and Pork”, *Indonesian Journal of Electrical Engineering and Computer Sciences*, vol.19, pp. 1626-1634, 2020.
- [23] J. Tan and J. Xu. "Applications of electronic nose (e-nose) and electronic tongue (e-tongue) in food quality-related properties determination: A review”, *Artificial Intelligence in Agriculture*. Vol. 4, pp.104-115, 2020.
- [24] K. Mahanti, Shivashankar, K. B. Chhetri, A. Kumar, B. Rao, J. Aravind, D. V. Swami, " Enhancing food authentication through E-nose and E-tongue technologies: Current trends and future directions”, *Trends in Food Science and Technology*. Vol. 150, pp. 1-26, 2024.
- [25] H. Syed, “Everyone just ate good food, Good food in Islamabad, Pakistan”, *Appetite*, vol.127, pp. 1-9, 2018.
- [26] N. Naeem, S. Raza, H. Mubeen, S. Siddiqui and R. Khokhar, "Food safety knowledge, attitude, and food handling practices of household women in Lahore”, *Journal of Food Safety*, Vol. 38, pp. 1-7, 2018.



**International Journal for
Electronic Crime Investigation**

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

DOI: <https://doi.org/10.54692/ijeci.2023.0803200>

Vol. 8 issue 3 Jul-Sep 2024

Advanced Techniques of Malware Evasion and Bypass in the Age of Antivirus

Kausar Parveen and Kinza Batool

Department of Computer Sciences, University of Engineering and Technology, Lahore

kbatool5121472@gmail.com

Received: Jul 06, 2024; **Accepted:** Jul 29, 2024; **Published:** Sep 12, 2024

ABSTRACT

The use of antivirus software as the main line of protection against growing cyber threats highlights the necessity of comprehending and resolving its limits. This study provides light on the ease of use and accessibility of tools used by hackers by carefully examining the complex terrain of malware evasion and bypass tactics. The persistent evolution of malware evasion and bypass techniques presents a significant cybersecurity challenge. The main objective is to educate users about the ever-changing hazards and provide them with the knowledge they need to properly strengthen their digital defenses. The literature analysis highlights the necessity for continued attention by establishing a strong correlation between the effectiveness of evasion strategies and their age and popularity. While modern antivirus software shows strong resistance against a range of tried-and-true techniques when updated on a regular basis, the study reveals a crucial component in its testing. This entails applying simple yet effective tweaks to well-known evasion techniques, demonstrating their capacity to fool even the most recent antivirus software. A thorough examination of malware evasion tactics, including both on-desk and in-memory approaches, is given in the methods section. Packing, obfuscators, protectors, reflective DLL injection, remote process memory injection, process hollowing, and inline hooking are all covered in detail in this paper. Subsequently, the study delves deeper into distinct evasion strategies, such as defensive evasion through direct system calls and sophisticated evasion tactics, showcasing malware developers' versatility in evading antivirus and endpoint detection and response (EDR) systems.

Keywords: Malware evasion, Malware bypass, Cybersecurity, antivirus, evasion.

1. INTRODUCTION

1.1. Opening Section

The widespread usage of the internet by many sectors of the population has made communication, entertainment, and information retrieval more convenient. But users that take advantage of this accessibility run the risk of being hacked by malicious software that compromises user privacy and sensitive data. As a major protection mechanism against cyberattacks, people frequently resort to antivirus software in reaction to this digital terrain. [1] Selecting trustworthy sources is crucial since downloading data from unknown sources can result in viruses, even with the widespread use of popular software like web browsers. Users can delete or clear suspicious files from quarantine by using antivirus applications, which are essential for alerting users about them. [2] The dependability of these defensive technologies depends on user confidence, which means that the antivirus program and its signature database need to be updated on a regular basis.

1.2. Background of the Research

Hackers are a constant danger to cybersecurity because they use a variety of evasion and bypassing techniques to access equipment without authorization. In order to meet this challenge, antivirus software providers are always creating new protection methods and upgrading signature databases. [3] On the other hand, the ongoing appearance of new viruses raises the possibility that the defenses in place now could not always be enough. By exploring the intricate world of malware evasion and bypass techniques, this study sheds insight on

how cyber threats are changing and highlights the need for creative solutions to strengthen digital defenses.

1.3. Statement of the Problem

The increasing complexity of malware evasion and bypass techniques poses a significant cybersecurity concern in the age of sophisticated antivirus programs. Concerns over the effectiveness of present defensive systems are raised by the rising number of new infections, and in spite of antivirus software vendors' constant attempts to create strong protection measures. The goal of this study is to thoroughly investigate the limitations of antivirus software, with a particular emphasis on the accessibility and usability of tools used by hackers. The goal of the research is to improve digital defense techniques by providing useful insights by comprehending and overcoming these constraints.

1.4. Rationale

The understanding of the dynamic nature of cyberthreats and the requirement for a proactive approach to cybersecurity serve as the foundation for this study. It is impossible to exaggerate the significance of having strong antivirus software in light of people's growing reliance on digital platforms. Through investigating the always changing strategies for evading and bypassing malware, [4] this study seeks to support continuous endeavors to fortify digital defenses. The results of the study will provide useful information for antivirus software manufacturers as well as users, resulting in a more robust cybersecurity environment.

1.5. Scope of the Study

This study is important because it may help users learn about the constantly evolving risks posed by cyberattacks

and provide them with the information, they need to strengthen their online defenses. Researchers have established a relationship between the popularity and age of evasion tactics and their efficiency, which is useful information for antivirus software producers as well as consumers. [5] The study's conclusions will further the current cybersecurity conversation by encouraging a more knowledgeable and proactive defense against changing cyberthreats.

1.6. Significance of the Study

This study is important because it may help users learn about the constantly evolving risks posed by cyberattacks and provide them with the information, they need to strengthen their online defenses. Researchers have established a relationship between the popularity and age of evasion tactics and their efficiency, [16,7] which is useful information for antivirus software producers as well as consumers. The study's conclusions will further the current cybersecurity conversation by encouraging a more knowledgeable and proactive defense against changing cyberthreats.

2. RELATED WORK

2.1. Literature Review

Installing antivirus software is seen as a crucial first step in safeguarding one's privacy on the internet. This literature study [1] however, explores the shortcomings of these products, emphasizing the ease of use and accessibility of techniques used by hackers to get around antivirus software. There is a significant association between the popularity and antiquity of evasion tools and their effectiveness, even though modern antivirus software that receives

frequent updates works well against them.

Interestingly, the study highlights default configuration weaknesses, showing that even the most recent antivirus software can be tricked by small changes to well-established evasion strategies. The study emphasizes the need for ongoing watchfulness since hackers use easily available resources to take advantage of potential vulnerabilities. The literature's ultimate goal is to increase user awareness of the hazards related to cybersecurity by advising them to stay vigilant and knowledgeable about the latest developments in digital threats.

Extending the research, the authors contrasted in a later paper the efficacy of antivirus software bypassing techniques on the Windows operating system with Kalogranis' work. In order to expand on their research, the authors included a new antivirus bypass tool dubbed TheFatRat [8], replicated the tests using the tools used by Kalogranis, and utilized a payload created with Metasploit. Shellter and Veil-Evasion were unable to get past security. Of the six antivirus applications that were employed, TheFatRat was able to bypass one (PeCloak.py 4) [9], whereas Avet was able to bypass five.

The research [10] chose to limit their testing to Bitdefender after reading an analysis of the antivirus software in another study, which ranked Bitdefender as one of the top options. The target PC was able to access the Remote Access Trojan (RAT) malware through the use of the Apache server. The authors examined nine different antivirus bypass methods, taking into account whether the antivirus program would be able to detect RAT as well as whether it would be able to prevent the

triggered Meterpreter session that RAT activated. As a fraction of the total number of ways for each tool, the effectiveness of these tools was displayed.

This paper [11] presents a new approach to return-oriented programming (ROP)-based code obfuscation. The two main aspects of ROP—automated analysis and creation of ROP chains for a given code and the repurposing of valid code as ROP gadgets—pose problems to standard malware research. The developed program, ROPInjector, uses executable code to patch the ROP chain and convert shellcode to its ROP equivalent. Experimental results on VirusTotals show that ROPInjector can bypass nearly every antivirus program, demonstrating the efficacy of ROP in obfuscating code. This study highlights the need for improved cybersecurity measures by highlighting the possible threat posed by ROP in cyberattack campaigns.

The research [12] concentrated on malware that can change its code on the fly to avoid detection, known as polymorphic malware. This method entails developing several malware variations, each with a unique code signature. Upon execution, the malware randomly chooses and runs one of the variations. Because each form of the malware has a different code signature, this makes it harder for antivirus software to detect the malware.

The literature study leads to the conclusion that, although antivirus software is not perfect, antivirus software bypass technologies do have benefits and drawbacks. The effectiveness of some antivirus software bypassing tools varies significantly, as has been observed.

This variation can be ascribed to a number of factors, including research methods, test dates, the type of malware being bypassed, its version, the tested antivirus software version, and even the collection of antivirus solutions that have been tested. Antivirus software and anti-virus software are engaged in a fierce competition in which the advantages of each side might have a substantial impact on the outcome.

As demonstrated, individual antivirus bypassing has been researched in the past for older antivirus versions. To the best of the author's knowledge, no thorough study has been done on the use of many antivirus bypass strategies together, nevertheless. Even while separate strategies have been researched and developed, it has not yet been investigated how efficient they are when combined. Considering the dynamic nature of malware and antivirus software, it is important to explore the ways in which different methods can be blended to get beyond several security levels. By better understanding antivirus software flaws, more resilient and efficient security measures may be created. This research can help.

2.2. Methodology

Malware evasion refers to strategies used to evade security system detection. This can involve using encryption to conceal dangerous payloads, polymorphic code that alters its appearance, and taking advantage of security software flaws. Avoiding detection frequently necessitates constant adjustment to security solutions' countermeasures. Malware evasion can be on disk or in memory.

more, so that they can avoid "Heuristic Detection," which makes it difficult for the program to understand the

instructions from antivirus software.

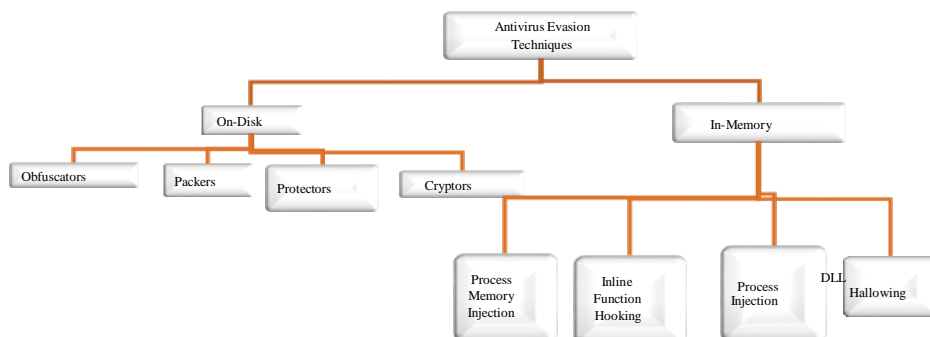


Figure 1. Types of Malware Evasion

2.2.1 Malware Evasion On-Disk

a) Packing

Malware is packed similarly to a compressed file, including new instructions and a larger file size to evade "signature-based detection."

b) Obfuscators

It obfuscates the blacklisted functions, such as VirtualAlloc, VirtualProtect, and more, so that they can avoid "Heuristic Detection," which makes it difficult for the program to understand the instructions from antivirus software.

c) Protectors

Although it complicates the malware's reverse engineering process, the Protectors app [3] is a regular one that wasn't intended for use in evasion, but it still has its uses.

Malware Evasion In-Memory

a) Remote Process Memory Injection

In order to apply this technique, we require certain APIs, such as: We inject our process or payload into a normal process like

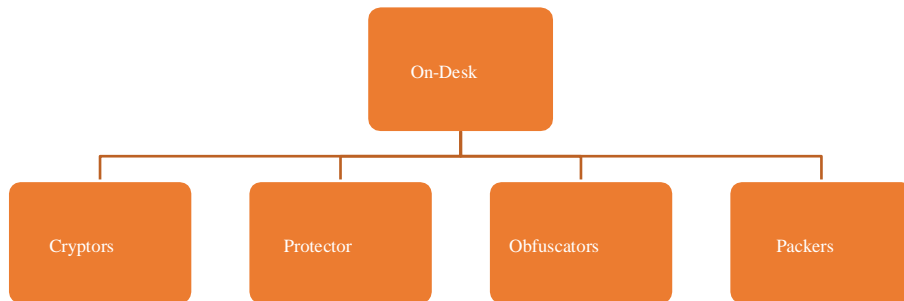


Figure 2: Showing Methods to Evade AV

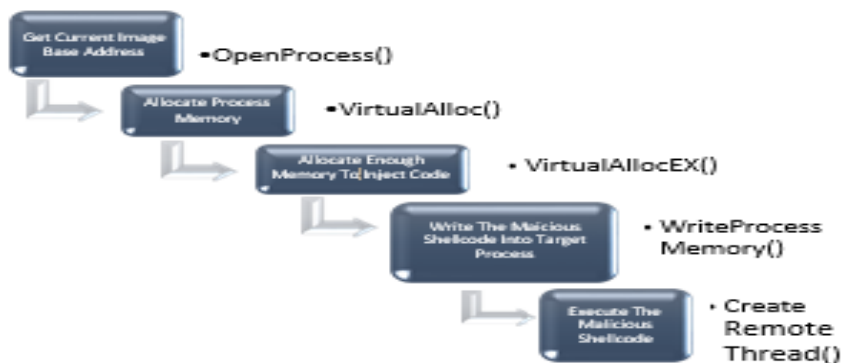


Figure 3: Common APIs for Remote Process Memory Injection

Reflective DLL Injection

An injection method that dispenses with using the conventional Windows APIs to load DLLs in order to load a DLL into the memory of a process. When limitations or security safeguards prevent the use of conventional DLL injection techniques, this can be helpful. The method by which

Reflective DLL Injection operates is called manual mapping. The fundamental idea is to execute the DLL directly from memory by mapping it there rather than utilizing the regular Windows API calls. As a result, the DLL can function without raising security alerts or drawing attention from antivirus programs.

b) Process hollowing

We create a fictitious process that consumes space, pause it, modify its content to match our payload, and then restart the process with his updated instructions and content.

A technique called "inline hooking" allows you to change a process's code while it's still executing in memory. Redirecting function calls from the original code to a new location in memory accomplishes this. Although there are other approaches, these are the well-known ones that are employed.

In the current digital era, cyber-attacks are a constantly changing concern. It's critical to stay one step ahead of attackers who are always coming up with new ways to get around established defenses. This research outlines the strategies employed by these attackers, with a particular emphasis on how they evade Endpoint Detection and Response systems. Certain malware can successfully evade detection by employing strategies like the usage of syscalls. These strategies go beyond the first infiltration phase. Attackers use sophisticated tactics like process injection and DLL hijacking to keep control of the system after they have gained access. Regarding analysis, 'Dark Crystel RAT (DCrat)' is highlighted as a leading illustration of contemporary cyber risks. Examining this danger in depth gives readers a thorough grasp of the difficulties this type of malware poses by illuminating how it operates. This information serves as a tool and is not merely academic. Individuals, companies, and organizations can better prepare and safeguard their digital assets in an increasingly hostile cyber environment by being aware of these hazards.

Techniques of Malware Evasion and Bypass

Following are the techniques used:

2.3.1. Technique 1

Defense Evasion Technique Using Direct Sys-calls and Advanced Evasion Methods

In order to escape AV/EDR detection, this strategy entails creating a suite of tools that utilize direct syscalls, evade sandboxes, employ strong encryption, and change procedure names. It also describes how to circumvent security protections and generate memory snapshots using the well-known utility Dumpert, which makes use of direct syscalls [6]. Notably, Microsoft Defender identified

Dumpert after it was created and utilized on the disk. This discovery prompted research into avoidance strategies for both static and dynamic scenarios.

It's essential to understand the specifics of Native APIs and Windows APIs. Applications run in user mode on Windows. They carry out operations using Windows APIs. Security solutions like AV/EDR can't view anything past the native APIs included in ntdll.dll. Consider malicious software that makes use of Windows API functions like WriteProcessMemory, CreateRemoteThread, and VirtualAllocEx. These APIs link to additional ntdll.dll API activities. The majority of the operations in ntdll.dll are sets of instruction steps that initiate kernel system level operations. AV/EDR tools often connect to Native APIs and modify the application's route whenever it performs these

activities, enabling them to detect potentially dangerous activity in the app. EDRs load their DLLs into the process memory at startup in order to monitor the actions of the application.

Defense Evasion Technique: A Two-Part Exploration

Part 1

Using native API function names, the syscalls are discussed in the first section. Next, to further complicate static analysis, the tool is enhanced with name changes. Creating ASM/H pairings with SysWhispers 2, which always utilizes random function names and determines syscalls as they change, is one step in setting up this evading detection technique.

his resolves the function hash into syscalls and make the call.

The native calls show up when you use IDA-PRO to perform a static analysis of the implant. These calls serve as markers of the binary's activity. With this combination, malware researchers may easily infer that the program is carrying out a process injection—a technique frequently used by malware creators for this very goal.

The method uses three sandbox evasion tactics in addition to encryption: determining the RAM capacity, determining the processing speed, and determining the number of core processors. The code above specifies that 8GB of RAM is required; the values for core processors and RAM capacity are adjustable. The application is meant to stop running right away if the RAM is discovered to be less than 4GB.

Even with the use of direct syscalls, which effectively get over most

AV/EDR solutions [13], there is still a need to improve the implant's stealth and resistance to analysis. AES encryption is used to further obscure against static analysis. Understanding that the well-known program msfvenom regularly generates shellcodes that are detected by AV/EDR systems, the shellcode was encrypted using AES to strengthen its stealthiness.

Part 2

To increase its stealth, the approach incorporates random naming for operations and functions, as was discussed in Part 1. For this reason, both the prototypes' names and the names of these operations were changed. Notably, prototypes of Native APIs are still easily recognizable even if they are not yet defined.

This version of the implant has function names that are chosen at random. This method is purposefully designed to make static analysis more difficult for malware experts. This foresight also takes into consideration possible future circumstances in which AV/EDR systems could identify the binary using these function names and the signatures that go along with them [14].

The methods were tested on Windows 11 by pitting them against McAfee, Microsoft Defender, and Kaspersky [15]. Surprisingly, none of these security measures were able to identify the implant, suggesting that the static and dynamic assessments required by these security measures were successfully circumvented.

The payload was integrated into explorer.exe. The payload's presence

can be observed within the memory address of explorer.exe, designated as RWX.

AntiScan was also used to evaluate the binary.me to assess the methods' effectiveness in detecting things. Remarkably, the binary escaped detection entirely.

By using randomized procedure names, strong encryption, sandbox evasion techniques, and direct syscalls, it was possible to successfully avoid EDR/XDR detection. In the final part, the strategy that may be used to go past Outflank's Dumpert tool is intended to be explained.

2.3.1.1. Bypass Dumpert Tool (Outflank)

Outflank created an amazing program that creates memory dumps by using straight syscalls. But because it's open-source, the majority of AV/EDRs have updated their signatures to support Dumpert. Instead of changing the signature, a different and more effective bypass technique was selected, with remarkable results. To begin with, @TheWover's tool 'Donut' was used to create an autonomous shellcode for Dumpert [16] in its raw form. All it takes to convert Dumpert.exe into raw shellcode is a simple command.

In order to avoid Dumpert's static analysis, in-memory execution is used. Although Dumpert's default method for creating memory dumps is through direct syscalls, an injector was also created to load Dumpert shellcode into a remote process. The same approaches that were previously mentioned are incorporated into this loader.

Because direct syscalls are incorporated into the injector to get beyond the user-mode hooking that AV/EDRs impose, this technique effectively gets around AV/EDRs.

2.3.2. Technique 2

Achieving Elevated Reverse Shells via DLL Hijacking and Mock Directories

The goal of this approach is to obtain a high-level privileged reverse shell by circumventing Windows UAC security features through the use of DLL Hijacking and Mock directories. The method, which security experts have identified, uses dummy files in conjunction with a simplified DLL hijacking procedure to get around UAC protections. Tests on Windows 10 were able to successfully disable the UAC security mechanism, raising concerns about how resistant Windows 11 is to similar tactics.

Escalating privileges is usually the next step after gaining initial access, with objectives such as hash dumping or performing [16] privileged actions that enable lateral movement inside a network. Think about a domain user who uses a PC and is also the local administrator. In the event that this user is compromised by an attacker, there is an instantaneous push to elevate privileges in order to dump hashes and utilize that user's NTLM hashes for network authentication. But since there is already an elevated reverse shell in place and a privileged connection to the C2 server established, there is no need for this kind of escalation. This method will explore the principles of DLL hijacking and identify particular Windows binaries that are helpful in executing this attack. The preferred instruments comprise Metasploit for

constructing.

Dynamic Link Libraries, or DLLs for short, are repositories of processes and code that facilitate Windows programs. Because they use the Portable Executable (PE) file type, they are similar to EXE files but cannot be executed directly. In

essence, DLL hijacking enables the insertion of malicious code into particular apps or services. This is accomplished by replacing the original DLL with a malicious one, making sure that the malicious DLL launches when the service is turned on. Because of the way certain Windows applications look for and load DLLs, such a swap becomes possible. When the DLL path of a service is not predefined in the system, Windows will automatically look for it in the environment path. By using this search pattern, attackers can place the rogue DLL in a location that Windows is aware of, preparing the way for the malicious code to be executed.

2.3.2.1. UAC – User Account Control

Initially included in Windows Vista and maintained in later iterations, UAC functions as a safeguard. Elevated rights cannot be provided to high-risk apps unless the user confirms it. Microsoft added "exceptions" to the UAC framework in an attempt [17] to improve user experience. This allowed trusted system DLLs stored in C:\Windows\System32\ to automatically rise to higher privileges without triggering a UAC question.

2.3.2.2. Mock Directories

In essence, a fake directory is a mimicked directory that can be identified by its trailing space.

Consider the Windows trustworthy directory "C:\Windows\System32."

The dummy equivalent would be "C:\Windows\System32," with the trailing space being the main distinction. Here, it's crucial to emphasize that Windows Explorer cannot be used to create mimic directories. PowerShell or the command prompt (cmd) must be used for creation. It is not possible to create "C:\Windows," however it is possible to set up "C:\Windows \System32."

2.3.2.3. TaskManager (taskmgr.exe)

Taskmgr.exe's integrity level was checked throughout the study. Taskmgr.exe is located in "C:\Windows\System32" and loads many DLL files when it runs. Attackers have the chance to use the DLL hijacking technique with this program [18]. This procedure "autoelevates" each DLL it introduces because of its high integrity level by design. It is possible to use many executables in a DLL hijacking attack [19]. "computerdefaults.exe" is the attack executable selected in this method. Attackers use these binaries to increase [20] their level of power in Windows, enabling them to perform DLL hijacking and change registry settings, among other things

2.3.2.4. Exploitation

This section explores the attack's mechanism, showing how an attacker may bypass Windows 11's UAC protections and acquire an administrator shell by using DLL hijacking and fake folders. This method's effectiveness was verified on Windows 11, even while Windows

Defender was turned on.

Steps:

1. Crafting a Malicious DLL Constructing
2. Mock Folder and Loading the Malicious DLL
3. Securing an Administrative Reverse Shell
4. Launching Mimikatz

To begin, a shellcode was formulated utilizing Msfvenom in the CSharp format, with Metasploit serving as the C2 server.

```
"Msfvenom -p windows/x64/shell_reverse_tcp  
lhost=0.0.0.0 lport=555 -f CSharp".
```

Following the creation of the shellcode, a straightforward C++ program was developed to produce a DLL file. This program incorporated the previously generated shellcode.

The next step is creating a batch program that creates fictitious folders, copies a file to one of these fictitious directories, and tries to load the malicious DLL. There are a number of ways to use Mimikatz and avoid Windows Defender detection. On the C2 server [6], user hashes were collected when Mimikatz was successfully launched. Numerous network-wide attacks may be carried out to authenticate users using these NTLM hashes.

2.3.3. Technique 3:

Direct System Calls for AV/EDR Evasion, User-Mode vs Kernel Mode

A variety of techniques are employed by contemporary AVs and EDRs to do both static and dynamic analysis. They may look at a variety of signatures, including keys, hashes, and recognized

strings, to find out if a file on disk is dangerous.

Nevertheless, attackers have created a wide range of obfuscation techniques, rendering static analysis all but useless. Dynamic/heuristic analysis is the primary emphasis of modern EDRs, which allows them to keep an eye on how each process behaves on the system and search for unusual activity. As a result, if malicious files have been disguised, this approach can download them and perhaps leave the EDR unnoticed [9]. However, as soon as the virus is activated, the EDR will recognize it and stop it. User-land hooks are used by the majority of AVs, EDRs, and sandboxes to monitor and intercept each user-land API call. They are unable to trace a technique that enters kernel mode and conducts a system call.

The fact that system call numbers differ between OS versions and occasionally even between service build numbers presents a problem. Nonetheless, the inmemory NTDLL module may be scanned to retrieve the syscall numbers using a library called inline syscall. The tricky part of this is that this module uses Windows API calls to retrieve the syscall number. These routines will not obtain the right number if an AV/EDR hooks them. Using Syswhispers is one alternate method that this blog discusses. By creating header/ASM files that implants can utilize to start direct system calls, SysWhispers helps in evasion.

2.3.3.1. SysWhispers1 vs SysWhispers2:

Although there is no requirement to specify which Windows versions to support, the usage is nearly comparable to that of SysWhispers1. Behind the scenes, most of the changes take place.

It no longer uses @j00ru's syscall tables and instead uses the @modexpblog-popularized "sorting by system call address" technique, which significantly reduces the size of the syscall stubs. The particular implementation in SysWhispers2 is a modification of the concept of @modexpblog. The function name hashes are randomized with every generation, which is one difference. Notable is also another version that was previewed previously by @ElephantSe4l and is built on C++17. Although it is still accessible, the original SysWhispers repository could eventually be retired.

2.3.3.2. API Hooks and Windows Architecture

AV/EDRs use a technique called "hooking" to intercept function calls and direct code flow to a controlled environment where the call's maliciousness may be examined. It is clear from looking at the Windows Architecture that a library by the name of NTDLL controls how user programs interact with the more complex OS operations.DLL.

The primary link between user-mode apps and the OS is the Native API (NTDLL.DLL). As a result, the OS serves as the interface between all applications. For example, ZwWriteFile and other frequently used Native APIs are stored in NTDLL.DLL. Several DLLs are loaded into a process's memory address space when it is started. When an AV/EDR loads a DLL, it can alter the function's assembly instructions by adding an unconditional jump at the start that points to the EDR's code.

Modern operating systems use multiple privilege levels and virtual memory to

isolate and separate running processes. Kernel-mode and user-mode are the two primary privilege levels recognized by the Windows operating system. Windows ensures that apps stay segregated and are unable to directly interact with system resources or critical memory regions by using this technique [18]. Direct access could be dangerous by nature and could cause problems with the system. The CPU switches to kernel mode when a program attempts to carry out a privileged job. Software can enter kernel mode thanks to syscalls, which makes it easier to do privileged tasks like writing files. Take the previously described Win32 API function WriteFile as an example. A process invokes the user-mode WriteFile function when it wants to write a file.

2.3.3.3. Injecting Shellcode Via Windows API

Standard techniques for inserting shellcode into a process are widely known to individuals who are knowledgeable about malware creation. Shellcode injection is frequently carried out by attackers using Windows API calls as VirtualAllocEx, WriteProcessMemory, and CreateRemoteThread. By using this procedure, a section of memory is created where the shellcode may be written. Then a remote thread is started, and the system waits for it to finish. A shellcode that would be inserted into the NOTEPAD.EXE process was created using msfvenom. This shellcode's goal is simple: it shows a message box with the words "Hello,

From Red Team Operator."
"Msfvenompwindows/x64/messagebo
x TEXT="Hi, From Red Team
Operator" -f csharp > output.txt.

This method introduces shellcode into a process by utilizing Windows APIs. The purpose of the presentation is to show that AV/EDR systems can identify such behaviors since they have hooks on these APIs. When memory is allocated to a process and marked as concurrently executable and writable, concerns are aroused. Since the shellcode is transcribed, executed, and created in memory using Windows APIs, it is obvious that AV/EDR systems would detect and flag these events.

2.3.3.4. Windows API Calls

This technique involves generating and injecting shellcode into notepad.exe. To achieve this, either the process name or the process id is required. Thus, the technique retrieves the pid of notepad.exe.

2.3.3.5. Shellcode Injection Through Syscalls

A program that writes the shellcode into the process and allocates memory via direct syscalls was created using the same previously produced shellcode. SysWhispers2, a program that dynamically resolves syscall numbers, was used. Due to SysWhispers1's reliance on the Windows operating system, SysWhispers2 was created and put to use.

The primary operating system for this method was Ubuntu, which posed a problem with the ASM/Header pair generated by SysWhispers2. There is a separate assembly format needed for compilation with Mingw64, and there is a distinct assembly format for

MASM. Conor Richard deserves recognition for reworking the current assembly, adding support for x86 (Wow64 & Native) and NASM ASM, and enabling compilation using MinGW and NASM straight from the command line. A malicious program was created [21] that inserts the shellcode—created by msfvenom—into the process using direct syscalls. This time around, all operations—including creating memory and inserting the shellcode into the remote process—are carried out using direct syscalls.

After successfully compiling and executing, program is caught by Windows Defender. Windows Defender discovered this method. The cause is that it made use of Windows APIs, which are often observed by antivirus and endpoint protection programs. These security tools make it easy to discover malicious programs that depend on Windows API calls to carry out such acts because they have hooks on user-land APIs.

Windows Defender discovered this method. The cause is that it made use of Windows APIs, which are often observed by antivirus and endpoint protection programs. These security tools may easily identify malicious applications that rely on Windows API calls to carry out such acts since they have hooks on user-land APIs.

Once the malware was successfully compiled, it was possible to avoid both static and dynamic detection by running the malware in the presence of Windows Defender. Within the project, this method used function names and random variables.

In the past, unsigned char shellcode was used for initialization while creating malware []. Windows Defender was

able to identify the infection as a result. The virus was identified by MDE as soon as it came into contact with the disk, even though it had encrypted the shellcode and masked API calls. Further analysis revealed that the detection was caused by the term ShellCode. As a result, it has been noted that antivirus software occasionally raises a warning based on these patterns. The virus dynamically modifies its variable and function names in order to thwart this and modify the static signature.

This time, Windows Defender did not detect the malware, as direct syscalls were employed. By leveraging [23] direct syscalls, it's possible to evade AV/EDR user-land hooking mechanisms.

This time, not a single antivirus program detected the malware once it was uploaded to AntiScan.me. The outcomes might be explained by the malware's anti-sandbox methods, which include examining CPU speed, RAM capacity, and processor count, or by the usage of direct syscalls. However, the virus was able to effectively avoid both static and dynamic analysis when tested against several AV/EDR solutions.

3. RESULTS

Significant new insights into the dynamic landscape of malware evasion and bypass tactics are provided by the research, which also highlights the continual innovation of measures that undermine the effectiveness of conventional antivirus software. Notably, the study emphasizes the necessity for creative defensive strategies by highlighting the shortcomings of antivirus software.

Testing contemporary antivirus software demonstrates its strong resilience to common evasion approaches, but the research also identifies flaws resulting from minute changes to tried-and-true tactics. The methodology thoroughly examines in-memory and on-desk evasion strategies, describing methods including packing, obfuscation, and reflection DLL injection. Advanced evasion techniques demonstrate the versatility of malware creators in avoiding detection. One such technique is defensive evasion via direct system calls. The effectiveness of combining encryption, random naming, and sandbox evasion to successfully evade AV/EDR systems is demonstrated by the results of particular evasion approaches. The research also looks at DLL hijacking and fake directories, which may be used to elevate reverse shells and cause issues with Windows UAC protection. Methods for AV/EDR evasion via direct system calls are shown, along with an overview of tools such as SysWhispers2 and the difficulties presented by contemporary security technologies. The study advocates for proactive defensive tactics and ongoing awareness in order to improve cyber resilience in the face of constantly changing cyber threats.

4. CONCLUSION

Proactive defense and awareness are crucial in the face of constantly changing cyberthreats. This study highlights the need for a comprehensive and constantly evolving strategy towards cybersecurity through its discussion of inventive methods and procedures. Conventional defenses still have their place, but ongoing learning

and adaptation are also necessary. This research seeks to provide people and organizations with the knowledge necessary to strengthen their digital defenses through its thorough examination. Let this research serve as a light for improved cyber resilience as we traverse this digital age.

5. REFERENCES

- [1] D. Samociuk, "Antivirus Evasions Methods in Modern Operating Systems," *Applied Sciences*, vol. 13, no. 8, pp. 5083, 2023.
- [2] D. Waterson, "Managing Endpoints, the Weakest Link in the Security Chain," *Network Security*, vol. 2020, no. 8, pp. 9-13, 2020.
- [3] S. Choi, T. Chang, S. Yoon, and Y. Park, "Hybrid Emulation for Bypassing Anti-Reversing Techniques and Analyzing Malware," *The Journal of Supercomputing*, vol. 77, no. 1, pp. 471-497, 2021.
- [4] S. Gold, "Advanced Evasion Techniques," *Network Security*, vol. 2011, no. 1, pp. 16-19, 2011.
- [5] D. Li, S. Cui, Y. Li, J. Xu, F. Xiao, and S. Xu, "PAD: Towards Principled Adversarial Malware Detection Against Evasion Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 1-16, 2023.
- [6] A. Monika and R. Eswari, "Prevention of Hidden Information Security Attacks by Neutralizing Stego-Malware," *Computers and Electrical Engineering*, vol. 101, pp. 79-90, 2022.
- [7] J. Cabrera-Arteaga, M. Monperrus, T. Toady, and B. Baudry, "WebAssembly Diversification for Malware Evasion," *Computers & Security*, vol. 131, pp. 32-43, 2023.
- [8] R. S. Kunwar, "Malware Analysis of Backdoor Creator: FATRAT," *International Journal of CyberSecurity and Digital Forensics*, vol. 7, no. 1, pp. 72-79, 2018.
- [9] "Evading Scanners," *The Antivirus Hacker's Handbook*, Wiley, pp. 133-164, 2015.
- [10] F. A. Garba, F. U. Yarima, K. I. Kunya, F. U. Abdullahi, A. A. Bello, A. Abba, and A. L. Musa, "Evaluating Antivirus Evasion Tools Against Bitdefender Antivirus," *Proceedings of the International Conference on FINTECH Opportunities and Challenges*, vol. 18, Karachi, Pakistan, 2021.
- [11] C. Ntantogian, G. Poullos, G. Karopoulos, and C. Xenakis, "Transforming Malicious Code to ROP Gadgets for Antivirus Evasion," *IET Information Security*, vol. 13, no. 6, pp. 570-578, 2019.
- [12] M. Christodorescu and S. Jha, "Static Analysis of Executables to Detect Malicious Patterns," *12th USENIX Security Symposium (USENIX Security 03)*, 2003.
- [13] D. Waterson, "Managing Endpoints, the Weakest Link in the Security Chain," *Network Security*, vol. 2020, no. 8, pp. 9-13, 2020.
- [14] H. Anand, N. Kumar, and S. K. Shukla, "Adversaries Strike Hard: Adversarial Attacks Against Malware Classifiers Using Dynamic API Calls as Features," *Electronics*, pp. 20-37, 2021.
- [15] M. Noor, H. Abbas, and W. B. Shahid, "Countering Cyber Threats for Industrial Applications: An Automated Approach for Malware Evasion Detection and Analysis," *Journal of Network and Computer Applications*, vol. 103, pp. 249-261, 2018.
- [16] M. A. Titov, A. G. Ivanov, and G. K. Moskatov, "An Adaptive Approach to Designing Antivirus Systems," *Safety of Computer Control Systems*

1992 (Safecomp' 92), pp. 215-220, Elsevier, 1992.

[17] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, "Orchestration of APT Malware Evasive Maneuvers Employed for Eluding Antivirus and Sandbox Defense," *Computers & Security*, vol. 115, pp. 10-28, 2022.

[18] H. Liu, W. Sun, N. Niu, and B. Wang, "MultiEvasion: Evasion Attacks Against Multiple Malware Detectors," 2022 IEEE Conference on Communications and Network Security (CNS), pp. 10-18, IEEE, 2022.

[19] J. Chen, C. Yuan, J. Li, D. Tian, R. Ma, and X. Jia, "ELAMD: An Ensemble Learning Framework for Adversarial Malware Defense," *Journal of Information Security and Applications*, vol. 75, pp. 103-114, 2023.

[20] T. Tsafrir, A. Cohen, E. Nir, and N. Nissim, "Efficient Feature Extraction Methodologies for Unknown MP4 Malware Detection Using Machine Learning Algorithms," *Expert Systems with Applications*, vol. 219, pp. 119-127, 2023.

[21] U. Ahmed, J. C. Lin, and G. Srivastava, "Mitigating Adversarial Evasion Attacks of Ransomware Using Ensemble Learning," *Computers and Electrical Engineering*, vol. 100, pp. 107-119, 2022.



Power of Homomorphic Encryption in Secure Data Processing

Muhammad Asif Ibrahim¹, Syed Khuram Hassan² and
Maham Akhtar

¹Department of Mathematics, The University of
Lahore, Lahore.

² Institute of Quality and Technology Management,
University of the Punjab, Lahore, Pakistan.

Corresponding author: khuramshah6515@gmail.com

Received: Jul 18, 2024; **Accepted:** Jul 30, 2024; **Published:** Sep 12, 2024

ABSTRACT

Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without first having to decrypt it. This paper presents a detailed discussion of HE, a critical component in the protection of data in today's technology-driven environment. First, homomorphic encryption and its terminology will be introduced and then development process from the beginning to the present state will be discussed. Different classes of homomorphic encryption and analysis of internal workings and architecture of homomorphic encryption will be discussed. The usefulness of this technology in ensuring privacy in sensitive areas is discussed, as well as the limitations that may hinder the technology's advancement, including computation intensity and data growth. The paper also reasserts the massive application of homomorphic encryption in data security and privacy, stressing the need to continue the advancement to overcome existing drawbacks and enhance the application of the technique. While moving vast distances within the digital arena, the optimization of homomorphic encryption remains the guiding light to our freedom and privacy online.

Keywords: Encryption, data, digital, homomorphic, protection

1. INTRODUCTION

In this digital era where data and information serve as bargaining chips

for malicious actors on platforms like the dark web, the need to protect these is increasing evermore as they have

formed an integral part of our lives. Data can literally be called the 'new gold' in this era. It is our property, one which encroaches deep upon our privacy and could significantly impact our lives if placed in the wrong hands. Our personal information, such as our name, gender, age, the websites we visit, and the words we search for in search engines like Google, etc., are all used to gauge our preferences and generate an online profile that is sold to advertisers [1]. While many companies may claim that they do not do this or that we consent to this operation once we agree to the 'Terms of Agreement,' the problem persists that we, as consumers, have limited control over what personal data is extracted, where it is sent and what is done with it. Even if we ignore the subject of the company whose services we are using, managing our data according to terms beneficial to them, there exists a chance that a malicious threat actor might hack the data placed on their servers and then auction it off to the black-market websites present on the dark web [2].

Many means have been adopted to counter security breaches, each with its respective pros and cons. The use of specific techniques, security software, and devices such as antivirus, firewalls, proxy servers, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), operating system hardening, frequent updating, use of VPN, Two Factor authentication, and backing up timely are some measures adopted for securing data. To protect data is to ensure that it remains confidential, maintains its integrity, is readily accessible when needed, and authentic, knows who created and

manipulated it, and ensures its existence to avoid any claim of disputation by any party. This is in line with the extended CIA triad in Information Security: to maintain Confidentiality, Integrity, Availability, authenticity, accountability, and non-repudiation. These principles are fundamental to protecting data and maintaining trust in digital systems. They help ensure that data remains secure, reliable, and verifiable, which is crucial in today's digital age.

2. SECURE DATA PROCESSING

One may adopt the approach of hardening defenses around the data to be protected; for example, think of a fort many kilometers tall with only one entrance at the bottom, whose keys are in possession of a few. The fort is surrounded by a deep moat, which can only be passed with the help of a draw bridge. This is a layering approach in which one must overcome different obstacles to reach the target. This corresponds to having your OS hardened, antivirus installed, system up to date, and firewall in place. The firewall is your first line of defense, just like the moat. The other approach is to make the target incomprehensible to unauthorized personnel. This involves using the technique of encryption. The objective of encryption is to protect the secrecy of data during both communication and storage, as noted by Caroline Fontaine et al. [1]. Even if it falls into the hands of an actor with malicious intent, the data would be of no use if it makes no sense.

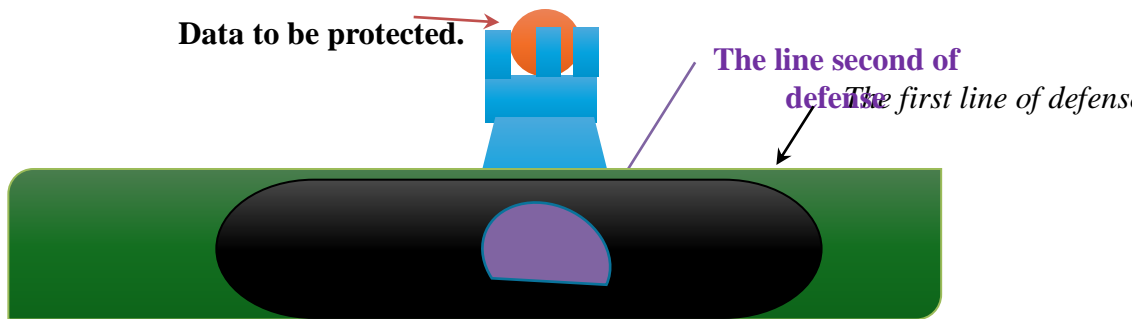


Figure 1: Analogy -A layered defense

But even with encrypted data, there are some concerns. For example, consider a scenario in which a party needs access to certain information placed on a server of another company to carry out tasks [3]. But a server contains more than just this information; it can contain sensitive, more personalized data. Hence, the concept of Homomorphic encryption comes into play. Computations are performed on encrypted data, and only the result is decrypted and sent back to the requestor. For consistency, the outcome after decryption must match the original computed value when applied to the initial data, as asserted by Caroline Fontaine et al. [1].

2.1. Homomorphic Encryption

The word 'Homomorphic' stems from Greek origin, comprising of 'homos' meaning 'same' and 'morphé' meaning 'shape.' In the field of abstract algebra, homomorphism is characterized as a mapping that retains all algebraic structures from the domain to the codomain within an algebraic set, as described by Abbas Acar et al. [2]. The map is simply a function, i.e., an operation, that takes the inputs from the set of domains and outputs an element

in the range (e.g., addition, multiplication). In the cryptography field, homomorphic encryption is used as an encryption type. Homomorphic Encryption (HE) represents a type of encryption that enables a third party, such as a cloud provider or service, to carry out specific calculations on encrypted data, maintaining the function's properties and the data's encrypted format, as indicated by Abbas Acar et al. [2]. Homomorphic encryption is similar to public key cryptography, i.e., asymmetric encryption, in that it utilizes more than one key but differs slightly. The concept shall be explained in more detail in the fifth section.

2.2. Encryption and its types

To encrypt something is to render it incomprehensible. This is done by performing specific steps or mathematical calculations on a given text and converting it into a puzzling mystery. The text upon which these operations are performed is referred to as 'plaintext' while the output is called 'ciphertext.' One of the very first forms of encryption was seen in 58 BC by the famous Roman General Julius Caesar, who used it as a secret means of

communication in his military. Called 'Caesar Cipher' after the renowned general, the Caesar Cipher is a form of substitution cipher where plaintext units are substituted with ciphertext following a predefined system. In this cipher, the alphabetic characters are shifted to a set number of positions in the alphabet, as defined by the 'key.' For instance, with a key of 3, the word 'HELLO' is encrypted to 'KHOOR' by shifting each letter three places forward in the alphabet.

2.2.1. Symmetric Encryption

The term “symmetric” implies that the same key is used for both encrypting and decrypting data. Therefore, it is necessary for both the sender and the receiver to concur on a shared key prior to initiating any secure communication, as mentioned by Abbas Acar et al. [2]. This means only the concerned parties have knowledge of the key. However, this key might be leaked during a transfer, i.e., when the two parties communicate and agree upon a key, this conversation might be intercepted.

2.2.2. Asymmetric Encryption

Public key cryptography was developed primarily to address the issue of secure key exchange and to ensure authenticity. One of the significant benefits of symmetric vital systems is that it eliminates the necessity for the parties involved in the communication to have prior knowledge of each other, enabling secure encrypted exchanges, as highlighted by Nigel Smart. Asymmetric encryption employs a pair of keys: a private key, which remains with the sender, and a public key, which is openly distributed. A message

encrypted with the private key necessitates its corresponding public key for decryption, and the same principle applies in reverse [2].

2.3. Lattice-based cryptography

Lattice-based cryptography, a variant of post-quantum cryptography, is predicated on the difficulty of solving specific lattice theory problems. A lattice is essentially a structured, repetitive pattern of points in a spatial arrangement. In cryptographic applications, these points are often depicted as vectors within a highly-dimensional space. Due to its discrete nature, there is a definable smallest element, aside from the zero vector, which is trivially the smallest by default. Many of the complex problems in computing, particularly in cryptography, are reducible to the task of finding the minor nonzero vector in a lattice, as stated by Nigel Smart [3]. Since it is a complex problem, it makes it difficult for an attacker to solve it to get the key.

Lattice-based cryptography has several advantages. They are gaining attention for their quantum resistance, positioning them as a viable substitute for existing public-key systems such as RSA and ECC, which are vulnerable to quantum computing attacks. Additionally, these cryptosystems offer advantageous features, including support for fully homomorphic encryption, enabling the execution of computations on data while it remains encrypted.

In two dimensions, you can think of a lattice as a grid of points on a piece of graph paper. Each point on the grid is an integer coordinate (x, y) , where x and y

are both integers. The points are evenly spaced along both the x and y axes. A 3D lattice can be visualized like a cube, where each vertex of the cube

represents a point in the Lattice. If you imagine stacking these cubes in a regular, repeating pattern along the x, y, and z axes, you would get a 3D lattice [4].

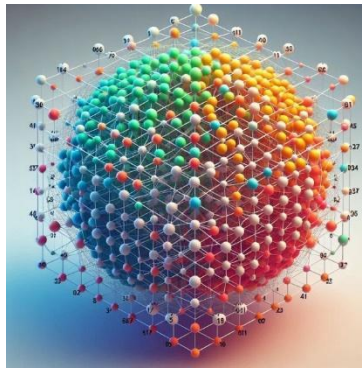


Figure 2: 3D Lattice

Each point in the Lattice has integer coordinates (x, y, z) and is evenly spaced along all three axes. The mathematical properties of lattices allow us to create encryption schemes that are currently unbreakable, even with the most powerful computers.

2.4. CVP and SVP Problems

The challenging issues linked with lattices, such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), play a crucial role in the robustness of encryption methods. For instance, within specific lattice-based encryption frameworks, the secret key is often a concise vector within the lattice structure. Decrypting a message requires solving the SVP to uncover this succinct vector. However, pinpointing the shortest vector within a lattice of high dimensions is a task of significant computational complexity, rendering the decryption process

exceedingly difficult for an adversary without knowledge of the secret key. Similarly, the CVP can be used in encryption schemes where the message is encoded as a point near the Lattice. To decrypt the message, you need to find the closest lattice point to this encoded point. Again, this is a complex problem, but it helps ensure the security of the encryption [5].

2.5. Certain types of attacks

Whatever encryption scheme is used, its goal is to be unbreakable. Hence, it should be able to withstand any attacks. Homomorphic Authenticated Encryption (HAE) is a cryptographic protocol that merges the functionalities of homomorphic encryption with those of authenticated encryption. It enables the execution of computations on encrypted data while simultaneously ensuring the integrity and authenticity of both the data and the computations,

all without the necessity of decrypting the data at any point.

In the context of encryption, a robust Homomorphic Authenticated Encryption (HAE) scheme must achieve indistinguishability under chosen plaintext attacks (IND-CPA) and ideally under chosen ciphertext attacks (IND-CCA), as defined by the standard find-then-guess scenarios according to Jeongsu Kim and colleagues [5]. Additionally, when functioning as an authentication mechanism, a secure HAE scheme is expected to be strongly unforgeable under both chosen plaintext attacks (SUF-CPA) and chosen ciphertext attacks (SUF-CCA), as detailed by Jeongsu Kim et al. [5]. These attacks are briefly explained below.

2.5.1. IND-CPA (Indistinguishability under Chosen Plaintext Attack)

This is an attribute of an encryption scheme whereby an attacker cannot gain any information about the plaintext if he/she is given two different ciphertexts. In other words, an adversary cannot distinguish between the two encrypted forms of two chosen plaintext messages.

2.5.2. IND-CCA (Indistinguishability under Ciphertext Attack)

This can be considered a more robust security measure in which an attacker cannot distinguish between the encrypted form of two chosen plaintexts even though he is allowed to decrypt more ciphertexts. This is to guarantee that even under more

complicated scenarios, the encryption scheme will remain concealed.

2.5.3. SUF-CPA – Strongly Unforgeable under Chosen Plaintext Attack

This characteristic of a digital signature protocol guarantees that even though an attacker has several signatures for the message, they cannot generate a new signature for a message they did not sign. It is crucial for security measures to help prevent the creation of new signatures without permission.

2.5.4. SUF-CCA (Strongly Unforgeable under Chosen Ciphertext attack)

This is a more robust security notion where, based on the signatures that are placed on a number of ciphertexts, an attacker cannot forge a valid signature on a new ciphertext.

2.5.5. Lattice Reduction

Lattice reduction attempts to convert a given lattice into a reasonable basis, which is pretty short and orthogonal. In the GGH cryptosystem framework, the selection of the public key from a “bad” lattice base and the secret key from a “good” lattice base is strategic. This approach is based on the premise that for lattices with a known “good” base, problems like the Closest Vector Problem (CVP) and the Shortest Vector Problem (SVP) can be resolved efficiently in polynomial time, as explained by Abbas Acar et al. [2].

3. PROGRESSION

Homomorphic Encryption has developed a lot since its early days. Homomorphic Encryption has been an area of continuing research and development. In the course of the development of cryptography, a range of homomorphic encryption derivatives, including partially homomorphic encryption, somewhat homomorphic encryption, and fully homomorphic encryption, has been identified. Every variant is characterized by a specific set of supported operations and overall operational effectiveness. At the moment, homomorphic encryption is one of the hot topics for investigation, especially as a means of protecting privacy in the contexts of cloud computing and secure multi-party computations. It is also used for cases where partial disclosure of data is not possible, but the data needs to be processed. Being used as one of the critical components of contemporary cryptography, homomorphic encryption enables the execution of operations on encrypted data, thus promoting the development of the field of data analysis and ensuring privacy.

3.1. Recent Developments

Wenju Xu and associates [6] have described Kumar and his colleagues' recent proposal of a novel noiseless FHE scheme using the Euler theorem. This proposed FHE scheme is quite unique for its efficiency in encryption, decryption, and homomorphic operations. However, it has been noted that the authors failed to present any proof of security or even a comprehensive security evaluation of their proposed scheme.

3.1. Certain Properties of Homomorphic Encryption

The properties of homomorphic encryption, such as Semantic Security or IND-CPA Security, Compactness, and Efficient Decryption, are important aspects of how it works. These characteristics are essential for their security, effectiveness, and feasibility. They facilitate the ability to carry out calculations on encrypted data, preserving confidentiality and avoiding the need for substantial computational power.

3.1.1. Semantic Security or IND-CPA Security

A homomorphic encryption framework is deemed secure when no potential attacker can determine (with more than a 50% probability) whether a specific ciphertext corresponds to the encryption of two distinct messages. To achieve this, the encryption process must be varied, ensuring that separate encryptions of an identical message appear dissimilar, as described by Melissa Chase et al. [7]. This means that the encryption is so strong that even if someone has the encrypted message, they cannot guess anything about the original message better than a random guess.

3.1.2. Compactness

This means that no matter the number of calculations that are made on the encrypted data, its volume does not change, thus, efficiency. An evaluator is capable of performing any number of supported evaluation functions and coming up with a ciphertext within the

ciphertext space, regardless of the complexity of the evaluated functions [8].

3.1.3. Efficient Decryption

The efficient decryption property of a homomorphic encryption scheme ensures that the time it takes to decrypt does not vary based on the complexity of the functions that were applied to the ciphertexts. In other words, regardless of the operations performed on the encrypted data, the decryption process remains consistently swift. This means that when performing the decryption of the encrypted data, the process is fast and cannot be determined by the number of calculations that were performed on the data. This makes it possible for you to be able to retrieve your original data quickly, as said by Melissa Chase et al. [7], irrespective of what was done to it when it was encrypted.

4. APPLICATIONS OF HOMOMORPHIC ENCRYPTION

Homomorphic encryption is pivotal in fields such as genomics, healthcare, national security, and education, as David Archer and colleagues emphasize [9]. Furthermore, Kundan Munjal and others have thoroughly examined and underscored its impact on the healthcare sector in a systematic review [10].

4.1. Healthcare

The data owners are Hospitals or Health Care Providers. The service latency is dependent on the cloud computing

resources, and the data volume is large (patient health records). The data is add-only, and the technical issues involve privacy and data security. The application of HE is possible now, with the main reason being the protection of sensitive medical information. The cost is expected to be borne by the healthcare providers. The cloud computing revolution has led to a demand for outsourcing applications. Users engage with the service by transferring their data to the cloud, where it undergoes processing, and they subsequently retrieve the processed results. This process is highly beneficial for the users; however, it also leaves their sensitive data vulnerable to exposure by third-party cloud service providers. Traditional encryption methods necessitate decrypting the data into its unencrypted state for computations, which poses a risk of disclosing sensitive medical information. Homomorphic Encryption (HE), as described by David Archer et al. [9] and Kundan Munjal et al. [10], offers a solution by enabling computations on data. At the same time, it remains encrypted, ensuring that only the encrypted form of the data is exposed to the service providers.

4.2. Genomics

Medical facilities, as the proprietors of data, can leverage homomorphic encryption to upload various genomic datasets to the cloud securely. This enables the delivery of tailored medical treatments, enhancing patient health and welfare. The expenses for these services are anticipated to be covered by health insurance providers [11].

4.3. National Security

In the event of a vehicular mishap necessitating the intervention of the city's emergency services, such as the Police, Fire Department, and several ambulances, the city's cloud infrastructure could promptly activate a server. This server would dispatch information solicitations to pertinent municipal divisions for instance, Police, Fire, Ambulance, and Transportation to allocate resources from each sector and devise optimal pathways from the accident location to appropriate medical facilities. The execution of these tasks demands diverse computational operations [12].

4.4. Education

The information employed in forecasting the likelihood of student dropouts is confidential and delicate. As such, encryption measures are essential to prevent any potential data breaches. Nonetheless, simply encrypting data while stored or during transfer is not adequate, as significant risks of data exposure persist throughout the processing phase [13].

4.5. E-Voting

Homomorphic encryption can increase the level of security and non-tampering of electronic voting systems. It allows the voter to verify the correct count of their votes and, at the same time, keep the voter's choice a secret. This approach could help increase the confidence of the people in the electoral process as well as the sanctity of election results [14].

4.6. Cloud-Based Systems

Homomorphic encryption is a very effective technique that provides security to the data stored in cloud systems. Since cloud storage means that data is stored on a server that many users can access, the data can be changed or even deleted. Homomorphic encryption safeguards this data since it can be processed in an encrypted form, and thus, the data is never revealed. This aids in the protection against unauthorized access and modification and can improve the users' confidence in the cloud storage services [13].

4.7. Machine Learning

Homomorphic encryption plays the role of an essential tool in enhancing the confidentiality and security of machine learning algorithms. It makes it possible to perform calculations on data that are encrypted to train and predict the next phase of a machine learning model without having to decode the actual data. It is most useful in situations where data security is of the essence, such as in the medical or finance fields. The model is able to learn from the data and provide accurate predictions, and at the same time, the data is protected. Therefore, homomorphic encryption is a powerful tool for machine learning that is focused on protecting data privacy [15].

4. CONCLUSION

Therefore, this paper has given a detailed analysis of homomorphic encryption, a significant component in a modern digital world where Cybersecurity is vital. In this paper, we have discussed the meaning of homomorphic encryption, its

background, categories, architecture, and practical use cases. However, homomorphic encryption is full of problems at the moment, such as computational costs and data blow-ups; however, it has great potential in the future. Thus, with the further enhancement of homomorphic encryption, the protection of our data in the age of digital development will be guaranteed, and our privacy will be preserved. Further research will be directed to the elimination of the present drawbacks and widening the usage of homomorphic encryption.

REFERENCES

- [1] C. Fontaine and F. Garland, "A Survey of Homomorphic Encryption for Nonspecialists," *EURASIP Journal on Information Security*, vol.7, 2007.
- [2] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," *ACM Computing Surveys*, vol. 51, no. 4, 2018.
- [3] N. P. Smart, *Cryptography: An Introduction*. New York, NY, USA: McGraw Hill, 2002.
- [4] V. Lyubashevsky, C. Peikert, and O. Regev, "On Ideal Lattices and Learning with Errors Over Rings," *Journal of the ACM (JACM)*, vol. 60, no. 6, 2013.
- [5] J. Kim and A. Yun, "Secure Fully Homomorphic Authenticated Encryption," *IEEE Access*, vol. 9, pp. 107279-107297, 2021.
- [6] W. Xu, Y. Zhan, Z. Wang, B. Wang, and Y. Ping, "Attack and Improvement on a Symmetric Fully Homomorphic Encryption Scheme," *IEEE Access*, vol. 7, pp. 68373-68379, 2019.
- [7] M. Chase, "Security of Homomorphic Encryption", *Proceedings of the Homomorphic Encryption Standardization Workshop, Microsoft Research, Redmond*, 2017.
- [8] G. Tu, W. Liu, T. Zhou, X. Yang, and F. Zhang, "Concise and Efficient Multi-Identity Fully Homomorphic Encryption Scheme," *IEEE Access*, 2024.
- [9] D. Archer, "Applications of Homomorphic Encryption," *Technical Report*, 2017.
- [10] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex and Intelligent Systems*, vol. 9, pp. 3759-3786, 2023.
- [11] I. Mustafa, H. Mustafa, A. T. Azar, S. Aslam, S. M. Mohsin, M. B. Qureshi, and N. Ashraf, "Noise Free Fully Homomorphic Encryption Scheme Over Non-Associative Algebra," *IEEE Access*, vol. 8, pp. 136524-136536, 2020.
- [12] M. Ogburn, C. Turner, and P. Dahal, "Homomorphic Encryption," in *Complex Adaptive Systems, Publication 3*, C. H. Dagli, Ed., pp. 502-509. 2013.
- [13] M. Li, "Leveled Certificateless Fully Homomorphic Encryption Schemes from Learning with Errors," *IEEE Access*, vol. 8, pp. 26749-26763, 2020.
- [14] T. Shen, F. Wang, K. Chen, K. Wang, and B. Li, "Efficient Leveled (Multi) Identity-Based Fully

Homomorphic Encryption Schemes,”
IEEE Access, vol. 7, pp. 84764-84775,
2019.

[15] R. L. Rivest, L. Adleman, and M.
Dertouzos, “On data banks and privacy
homomorphisms,” *Foundations*
Secure Computation, vol. 4, no. 11, pp.
169-180, 1978.



Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

Ghulam Abbas¹, Ghulam Rasul Zahid², Abdullah Hassan Hashmi³, Maiha Kamal⁴, M. A. Naveed¹, S. Jaffery⁵, Mazdar ul Hassan¹, M. Imran⁷, Ahsan Mustafa¹, Humaira Farah⁶, U. Farooq⁸, U. Mahmood⁸, M. F. Khalid⁸, M. Auon⁸

¹Riphah College of Veterinary Sciences, Riphah International University Lahore, Pakistan

²Police Service of Pakistan, Joint Director General Intelligence Bureau Islamabad, Pakistan

³University Institute of Food Science and Technology, University of Lahore, Pakistan.

⁴Department of Mass Communication, Government College University, Faisalabad, Punjab, Pakistan.

⁵Faculty of Agriculture, University of Agriculture Faisalabad, Pakistan

⁶Department of Sports Sciences and Physical Education, University of Lahore, Pakistan

⁷Pet Centre, University of Veterinary and Animal Sciences, Lahore

⁸University of Agriculture Faisalabad, Sub campus Toba Tek Singh, Pakistan.

*Corresponding Authors: ghulamabbas_hashmi@yahoo.com

Received: Jul 19, 2024; Accepted: Aug 02, 2024; Published: Sep 12, 2024

ABSTRACT

The rise of digital technology and social networks has caused an increased rate of cyberbullying cases, predominantly among adolescents. Problematic use of the internet and cyberbullying have had important psychological, social, and emotional impacts on youth, making it a tenacious concern for educators, parents, and policymakers. Effective parent-adolescent/youth communication arises as an essential approach to alleviating the risks and effects of cyberbullying. This review study aims to explore the role of open and helpful communication between youth and parents to avoid cyberbullying. Investigating the various communication approaches and their effect on youthful behavior, the review augments the importance of adopting a helpful and thoughtful environment at homes and educational institutes. The review suggests that youths who are involved in regular frank discussions with parents and teachers about online activities are less prone to cyberbullying. Moreover, the study stresses the need for parents and teachers to be well-familiar with digital/social platforms and cyberbullying dynamics to successfully guide the youth. Educating the parents, teachers,

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

and youth aimed at enlightening communication skills amongst youths, parents and teachers demonstrates promise in decreasing the cyberbullying cases in Pakistan. Therefore, this manuscript intends to explore approaches that involve universities, digital platforms, and communities to support parent-adolescent communication to create safe online environments for the youth.

Keywords: Digital technology, social networks, cyberbullying, youth, universities, parent-adolescent communication.

1. INTRODUCTION

Navigating the variety of digital challenges that today's youth face requires a comprehensive strategy. A complex online environment is created by factors such as cyberbullying, peer pressure, social media pressure, online privacy issues, academic pressures, mental health effects, and changing peer relationships. It is the responsibility of parents, teachers, and the community at large to promote responsible digital use, encourage open communication, and offer direction. The young generation needs to be taught how to positively exploit digital technology while reducing any possible risks by tackling these problems head-on. It is found that parental communication with teenagers protects them from cyberbullying. Students who had not experienced cyberbullying are reported more likely to have open contact with their parents, according to a study done on high school students in Valencia, Spain. Students who had occasionally or severely experienced cyberbullying were more likely to engage in avoidant communication. Beyond the consequences of parents' online supervision, there was a negative correlation between cyberbullying victimization and perpetration and parent-child connectivity as indicated by open communication. This shows that having a solid relationship with honest communication may be more crucial

than keeping an eye on young people's internet activity [1, 2].

Communication between parents and children has its key significance in preventing cyberbullying and safeguarding against its adverse consequences. For example, parents purposefully allowed their kids to see things in their way when cyberbullying happened in the southern United States. Additionally, they wished for their kids to understand the possible causes of cyberbullying i.e. dysfunctional families and lowered self-esteem. Parents also used communication techniques to give their kids more authority. They introduced to their kids the value of resisting bullies and standing up for others who are weak. They also attempted to foster a feeling of self-assurance in their skills. A qualitative study is required to comprehend how parents' techniques may differ from those of parents in Western cultures, given the emphasis on collective interdependence in Eastern cultures, such as India [3].

Talking to parents is a useful coping mechanism when students are facing cyberbullying, however, Cassidy et al. found a disparity between adolescent reports of cyberbullying (32% victimization: 36% perpetration) and parents' understanding of cyberbullying (11% aware of cyberbullying events) in a mixed methods research of parents and children (6th – 9th grade) in England. These results suggest that young people don't always tell their parents about

incidents of online harassment. The study also showed that parents thought they could enforce rules more strictly and that their children were engaging in less cyberbullying than the young people reported. In a follow-up study, the researchers discovered that the degree to which parents were ignorant of their children's Internet usage both positively correlated and predicted the behaviors of cyberbullying. Young people may choose not to ask for adult assistance because they don't think adults can effectively step in or because they worry about losing access to their electronics. Without adult assistance, young people are more prone to resort to unhealthy coping mechanisms like avoidance, turning into cyberbullies themselves, or taking violent revenge on the offender(s). All of these could contribute to an increase in cyberbullying [4, 5, 6].

Vignettes can draw attention to challenges in distinguishing between acceptable and inappropriate use of social media and the Internet. As is often the case with human behavior, there is a spectrum that spans Internet use from normal to problematic [7, 8, 9]. Parents, teachers, and clinicians may find it difficult to distinguish between normal and problematic online activity when 95% of US teens go online daily and 45% go online almost constantly [10]. Additionally, adolescents frequently engage in media multitasking, with over 50% engaging in multiple media activities at a given time, such as being online and watching TV [11]. Overuse of the Internet in kids has been linked to anxiety and depression, difficulty sleeping, poor academic performance, difficulty adjusting to social situations, and even a higher risk of suicide [12, 13, 14, 15].

The 18-item Problematic and Risky Internet Usage Screening Scale (PRIUSS-18) evaluates social impairment, emotional impairment, and risky/impulsive Internet

usage, therefore, standardized and accurate screening is essential for adolescent and young adult populations [16, 17, 18, 19]. Using a 5-item measure (never = 0, seldom = 1, occasionally = 2, often = 3, very often = 4), individuals who score 25 or higher are considered to be at risk for PRIU. Compared to use for business or education, there is a stronger correlation between PRIU symptoms and leisure Internet use. It should come as no surprise that individuals with symptoms of inattention had the strongest correlation with the risky/impulsive usage domain.

A variety of parenting techniques are recommended by experts to reduce cyberbullying and improve internet safety. Parenting at its most successful might involve putting a lot of focus on autonomy and active media monitoring. -According to O'Connor et al. [20], media parenting is defined as "goal-directed parent behaviors or interactions with their child about media to influence some aspect of the youth's screen media use behaviors." Throughout adolescence, parents and children naturally work out boundaries—including restrictions on online activities—as children want to become more independent and parents want to protect them. Parents and children display a diversity of patterns in these talks, but households, where parents exert high control and adolescents, push for high autonomy are likely to experience the most conflict [21]. A balanced approach may be best, as one study found that youth who reported high levels of parental control were also likely to report high levels of cyberbullying [22]. In another study, Padilla-Walker et al. found that autonomy-supportive media parenting (whether active or restrictive) was associated with high media disclosure. Finally, the study found that when children voluntarily tell their parents about their online activities, they

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

tend to engage in more pro-social activities and less relational aggression [23].

Research focusing on the consequences of cyberbullying has also revealed potential safeguards for media parenting practices, like keeping an eye on their children's online activity. Using technology controls or house rules to limit media consumption is one example of restrictive parenting. According to research by the Pew Institute, most parents keep an eye on their teenagers on social media (up to 61%) and frequently check their calls or texts (48%). Parent-child conversations on media usage and active media use together, or co-use, are referred to as active mediation [24, 25, 26]. Parents are less likely to actively teach or discuss online behavior with their teens (40%) than they are when it comes to restrictive media parenting.

2. REVIEW OF LITERATURE

The literature shows that there are differing opinions about the effects of restrictive media monitoring on cyberbullying. This can be the case because parents may set greater boundaries if they are aware of cyberbullying. Restrictive media monitoring was found to be less beneficial in longitudinal research than parent-child communication and connective co-use, or the active use of media together. Open communication such as asking someone where they're going tonight may be necessary when monitoring in person. "Who will you be with?" while internet surveillance can be carried out in silence (e.g., by watching videos on TikTok or by following accounts on Instagram without leaving comments). Some teenagers have indeed shown anger on social media when their father follows them or their pals [27]. Supporting autonomy at the same time may be essential to restrictive parenting

techniques. Autonomy is a fundamental concept in the Model for Cyberbullying Motivation and Regulation. Children would be able to develop and learn if there was active dialogue and negotiation over media, especially as they got older. Empathy and self-control are fostered by active media parenting, and these traits have been linked to a decrease in aggressive and externalizing behavior as well as an increase in pro-social behavior. In general, positive parent-child interactions, open communication, and active media parenting are essential when paired with certain realistic limitations, including parental phone limits for young teenagers. However, placing too much focus on limitation and control can have unintended consequences [28].

Recognizing that the majority of teens and young adults live their lives online and that technological literacy is essential for their ability to function in the workplace, play, and academic settings would be a good place to start [29]. Accurately recording online behaviors and the related health and risk variables is one of the issues. Media use provides a wealth of information about patients, including their time management skills, interests, and desired public image. It also reveals information about their understanding of privacy settings, propensity for risky behavior, executive functioning, and behavior consequences awareness. Additionally, it provides an overview of their familial ties, uninspiringly features of their Internet use, number and quality of relationships, and cultural self-identification.

Clinicians establish a trusting relationship with patients/students to discuss their internet use habits openly [30], ensuring that patients/students feel comfortable and non-judged whilst discussing their internet habits [31] and employ validated assessment tools to quantify the degree of PIU [32]. Assess the physical and mental health influences of

extreme internet usage, like depression, sleep disturbances, and anxiety [33]. Clinicians give tips and guidelines for healthy usage of the internet [34] and explain the potential risks of excessive internet use and its consequences like addiction and its effect on mental health [35]. They create modified treatment strategies based on the precise needs and situations of each patient [36], psychoanalysis services, and support groups to help persons manage their internet use [37]. Educators recognize signs of unnecessary internet use and discuss the patterns of internet usage and its effects on routine life [38], i.e. social withdrawal or declining

academic achievement [39]. Educators keep an eye on the academic performance of students and their social interactions to recognize potential issues [40]. They administer reviews to collect data on students' internet use [41] and combine training on digital literacy into the curriculum to help students understand the importance of balanced internet use [42] see Table 1. Educators inspire a balanced lifestyle that comprises physical activities and offline social communications [43] with the help of parents or guardians they support habits of healthy internet use in students [44] and implement broad programs within schools to motivate beneficial internet use and digital well-being [45].

Table 1: An approach for clinicians and educators to engage, assess, educate, and treat problematic internet use

Step	Role	Actions	Consequences
Engage	Clinicians	Build rapport with students or patients [46]	Create a non-judgmental but safe environment [47]
	Educators	Recognize signs of excessive internet use [48]	Start conversations about internet habits [49]
Assess	Clinicians	Conduct thorough evaluations using standardized tools [50]	Assess mental and physical health impact [51]
	Educators	Monitor academic performance and social interactions [52]	- Use surveys and questionnaires [53]
Educate	Clinicians	- Provide information on healthy internet use [54]	- Discuss risks associated with excessive use [55]
	Educators	- Integrate digital literacy into the curriculum [56]	- Promote awareness about a balanced lifestyle [57]
Treat	Clinicians	- Develop individualized treatment plans [58]	Offer counseling and support groups [59]
	Educators	- Collaborate with parents and guardians [60]	Implement school-wide programs [61]

Table 2: key aspects of establishing a therapeutic alliance with a young adult patient

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

Aspect	Individual Therapeutic Alliance	Alliance with Patients and Parents	References
Trust Building	Create a safe, confidential environment for open dialogue.	Foster transparency about the therapeutic process while respecting confidentiality.	[64, 65]
Active Listening	Validate the patient's feelings and concerns.	Encourage parents to listen to the patient's perspective without judgment.	[66, 67]
Goal Setting	Collaboratively set personal goals for therapy.	Involve both patient and parents in discussing goals, ensuring they are realistic and mutually agreed upon.	[68]
Communication	Use age-appropriate language and be mindful of non-verbal cues.	Facilitate open communication, encouraging questions and clarifications from both parties.	[69]
Empowerment	Encourage self-efficacy and independence in decision-making.	Support the patient's independence while educating parents about their support role.	[70]
Conflict Resolution	Address any misunderstandings directly and constructively.	Mediate discussions to resolve conflicts, focusing on the patient's needs and feelings.	[71]
Feedback Mechanisms	Regularly solicit feedback on the therapeutic process and adjust accordingly.	Create a forum for feedback that includes both patients and parents to ensure all voices are heard.	[72]
Cultural Sensitivity	Acknowledge and respect the patient's background and beliefs.	Recognize family dynamics and cultural factors that may influence treatment and interactions.	[73]
Follow-Up	Schedule regular sessions to maintain continuity of care.	Encourage family involvement in follow-up discussions to reinforce support outside therapy.	[74]
Confidentiality Respect	Maintain patient confidentiality to build trust.	Clarify the limits of confidentiality, especially regarding safety concerns or legal requirements.	[75]

Establishing a therapeutic alliance with a young adult patient on an individual basis or with the patient and their parents is the first stage (see Table 2) Involvement between the patient and the physician, a therapeutic alliance that involves the youngster and the parent, and joint treatment decision-making are all necessary for providing high-quality care in psychiatry [62]. Given that many adults and young people view the Internet as their only means of interacting with others, discussion of the negative elements of Internet use may be met with resistance. To fully comprehend and address each patient's needs, it is essential to investigate their beliefs, norms, values, cultural and linguistic context, and personal interpretations of technology [63].

Presently, the digital platform presents numerous challenges that have considerably affected the well-being and mental health of our youth. Online harassment and Cyberbullying have become widespread painful issues in our society, worsened by obscurity and internet access, resulting in severe psychological distress and anxiety. Digital media platforms, no doubt offer ways of self-expression, yet they impose naïve beauty standards and substitute negative body image insights. Understanding the complex digital challenges is an indispensable step for nurturing a healthy and balanced contact with technology. Cyberbullying is one of the main problems with technology that teenagers are facing. Due to the widespread use of social media, places intended for communication have become havens for harassment. Cyberbullying can take many different forms, from nasty remarks to the dissemination of false information. It has a detrimental effect on teenagers' mental health by encouraging emotions of loneliness, anxiety, and sadness. Social media's well-manicured

exterior places pressure and unreasonable expectations on teenagers. Body image issues and low self-esteem are frequently caused by exposure to images of "perfect" bodies, lives, and experiences. One digital barrier that kids face as they try to fit into an idealized online world is the desire for affirmation through likes and comments.

As more teenagers reveal personal information online, the growing problem of online privacy becomes more pressing. People are exposed to possible risks like identity theft and online predators since it is difficult to distinguish between appropriate sharing and excessive sharing. For today's youngsters, finding a balance between protecting privacy and keeping up a digital presence is a constant problem. Technology has transformed schooling, but it has also presented new challenges for teenagers. Study habits and attention are hindered by the ubiquitous connectivity that laptops and cell phones provide. Teenagers attempting to satisfy academic expectations face a challenging environment as a result of the culture of comparison fostered by social media and the pressure to perform academically. Teens who spend too much time on screens face two problems. Even though technology provides a wealth of educational and recreational opportunities, extended screen time negatively affects mental health by raising stress levels, upsetting sleep cycles, and increasing stress levels. For teenagers in the digital age, finding a balance between using technology for enrichment and giving mental health priority is still a constant struggle. Teenage relationships now face new challenges as a result of the digital age, such as navigating online romantic interests and forming connections with peers across the globe. Key components of teenagers' digital journeys include comprehending the nuances of online

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

communication and differentiating between genuine connections and surface-level exchanges.

Internet usage can range from beneficial to detrimental. Psychiatric educators need to learn about technology to help trainees gain clinical expertise in assessing patients, particularly PIU. A comprehensive media history is a crucial part of a mental health assessment, particularly for adolescents and tweens. Several informers, such as parents, teachers, the youngster's primary care physician, and/or other people who are familiar with the young person can help to improve the assessment of the youth hence standardizing media usage as most normal people do, nevertheless, is also crucial.

It's important to have an open-minded conversation with parents and youth about the variety of use from healthy to hazardous. [76]. To address the health, education, and entertainment needs of each child as well as the needs of the entire family, the American Academy of Pediatrics, for instance, has developed the Media and Communication Toolkit and Family Media Use Plan, which emphasizes the family as a whole and may be less difficult and offending. Numerous aspects i.e. the patient's behavior or problems make evaluation difficult [77], which depends on the patient's age and progressive stage. The growing brain may be more affected by technology than the mature brain [78]. Highly problematic online usage and "internet gaming disorder" have been proposed as a condition that needs vast study. "Gaming disorder" has recently been included in the 11th Revision of the International Classification of Diseases (ICD-11) classification framework. It's characterized by a pattern of gaming behavior (i.e., digital/video gaming) that includes losing control over gaming, giving

gaming more importance than other activities to the point where it trumps interests and daily activities, and continuing or increasing gaming even in the face of negative outcomes.

The Internet use intensity and other factors, including peer habits, family rules and expectations, technology availability, and environmental aspects of the individual, should be assessed by the clinician to better understand the factors that support or sustain problematic use of the internet. This is because Internet use is in a state of dynamic interaction with contextual and activity-related factors. When it's appropriate, asking patients whether they would want to show doctors examples of their social media posts can help clinicians learn more about their hobbies, morals, and routines. In general, broad measures about behaviors, time spent using/exposure to technology, and exposure to "content" are required. Standardized examinations are frequently used in studies that examine how technology affects academic success and other behaviors [79].

Educating the patients about appropriate internet use and the risks associated with excessive screen time (i.e. disturbed sleep, worse academic and social performance, and a worsening of pre-existing psychopathology) is beneficial to youth and families. Arranging motivational interviewing techniques can help in collaboratively creating a strategy that aligns with the patient's goals and values (see Table 3). Determining the factors/procedures that resist excessive internet use is beneficial to boost the mental health of students. If a treatment plan outlines substitute activities that could satisfy excessive and overuse of internet activities' emotional requirements, it can play a high role in combating the curse.

Table 3: Education, advice, and treatment principles for excessive use of the Internet

Aspect	Description
Education	Provide information about healthy internet use and the risks associated with excessive use.
Awareness Building	Encourage self-reflection on internet habits and their impact on daily life.
Setting Limits	Help individuals establish boundaries on daily internet use to promote balance.
Coping Strategies	Teach alternative coping mechanisms for stress and boredom that do not involve internet use.
Support Systems	Encourage involvement in social activities and offline relationships for emotional support.
Professional Help	Recommend seeking therapy or counseling for severe cases of internet addiction.
Skill Development	Foster skills in time management and self-discipline to reduce excessive use.
Monitoring Tools	Suggest the use of apps and tools that track internet usage to raise awareness of habits.
Digital Detox	Encourage periodic breaks from the internet to reset habits and improve well-being.
Community Programs	Promote participation in community or support groups for shared experiences and strategies.

3. CYBERBULLYING A CHALLENGING ISSUE

Disinhibiting and the sharing of inappropriate images are two examples of problematic social media activities. More extreme instances include cyberbullying, online bullying, sexting, straightforward exploitation, and other addictive behaviors [80]. Sending, receiving, or sharing explicit messages, photos, or other visuals that contain sexually suggestive information is known as sexting. This can happen in conversations between persons who are not yet in a relationship, between romantic partners, and/or between people who are not in a primary relationship. As the number of devices with Internet connection has increased, sexting has grown more widespread. Although it is practiced by people of all ages, the majority of media attention concentrates on the negative effects on tweens, teenagers, and young adults, who use text messaging more than any other new media to communicate sexually explicit messages [81].

Ultimately, however, there is still disagreement over the terminology, so reaching a consensus is crucial to accurately assessing the activity and modifying prevention [82].

Scientific research has produced a wealth of information about bullying and cyberbullying, and teenagers who are reported experiencing online bullying are increasingly alerting i.e. 60% in 2014 compared to 40% in 2013. Cyberbullying is the deliberate and persistent harm (e.g. threatening, dehumanizing, or harassing text messages or photographs) sent via mobile phones, interactive technology, or the Internet . More than 40% of American teenagers (of the age group between 13-17 years) said that they had been the victim of cyberbullying at some point in the previous year. On the other hand, 11.5% of teenagers acknowledged engaging in cyberbullying. The likelihood of cyberbullying victims is higher for girls (>40%) compared to boys (29%). Boys are more likely to play video games than girls, but girls also dominate social media. In severe circumstances, peer

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

victimization brought on by cyberbullying has a clear correlation with a higher risk of suicide. Compared to traditional bullying, being the victim of cyberbullying has a stronger correlation with suicide ideation. Teens are not the only ones affected by this problem. According to a recent meta-analysis, this phenomenon holds for both younger and older kids, males and girls, and kids who bullied and were bullied themselves. For kids in grades 3-5, simply having a cell phone greatly raises the risk of cyberbullying [83].

Around the world, 72% of teenagers game online. Playing video games is a common pastime for kids and young adults. Online and in-person pals can play a lot of video games, regardless of whether they are console, web, or computer-based. The ability to create alter egos or fictional versions of oneself is made possible by the perceived anonymity of players and the use of avatars. This feature of gaming is fun, but it also allows users to harass, bully, and occasionally group up with other players by sending or posting hurtful or negative messages and using the game as a tool for harassment. When a child doesn't perform well, other kids might curse at them, make cruel comments that escalate into bullying, or stop them from playing altogether. Anonymous players might use the game to harass strangers or obtain private information about them, such as usernames and passwords [84].

Parents and adults should learn how the game operates and what kind of content a child is exposed to, play it yourself, or watch others while they play to stop children from being cyberbullied while they are gaming. Moreover, parents/teachers should talk to their children/students regularly about who is playing the game with them and who is online. Further, instruct young people in safe online conduct, such as avoiding

clicking on links from strangers, keeping personal information private, abstaining from other players' bullying, and knowing what to do if they witness or are the victim of bullying. Set limits on how much time a kid or adolescent can spend playing video games.

Many victims have limited information on how to report cyberbullying and existing laws are not sufficient or effectively enforced. Therefore, victims feel ashamed/fear social repercussions thus high-risk behaviors may be seen as a way to fit in with peers due to insufficient access to mental health services [82]. Mental health-related issues are often stigmatized, and discourage patients from seeking help, hence continuous excessive usage of the internet results in addiction. Undue online activities result in boredom from study as students like to spend more time in their favorite online interests. Prolonged screen time causes physical health problems such as eye strain.

Cyberbullying, high-risk behaviors, and excess online activity can be prevented through policy changes, education, and accessible support systems. For this, there is a dire need to implement effective programs in universities/colleges/schools to educate students about the devastating effects of cyberbullying and how to prevent it. Updating and strictly enforcing cybercrime laws can help to discourage cyberbullying. Moreover, provide confidential support services for victims and conduct campaigns to educate about the concerns of high-risk behaviors for good control of Cyberbullying, high-risk behaviors, and excess online activity, increased support services and mental health counseling may helpfully Educate individuals about maintaining a healthy balance between online and offline activities, hence, promote open and de-stigmatized discussions about mental

health. Encourage setting limits on screen time to avoid negative impacts on academics and health. Implement programs that promote periodic breaks from digital devices to improve overall well-being [85].

CONCLUSION

The present study emphasizes the key role of parent-adolescent communication in preventing cyberbullying among youth. Effective communication serves as a protective factor, equipping adolescents with the necessary skills and knowledge to navigate safely the digital world. Yet, parents who keep an open communication, express frank interest in the online activities of their children, and guide them without being unpleasant raise a sense of security and trust. This environment allows youth to get support and motivation to report cyberbullying cases, decreasing the possibility of long-term retaliatory behavior. Various approaches like resources and educational programs that can enhance parental alertness of cyberbullying and digital learning can play significant roles in combating this dangerous issue. These motivations may focus on training parents with practical approaches to be involved in critical conversations about probable risks related to digital communications, online behavior, and privacy. Moreover, promoting a cooperative approach that comprises the collective effort of universities, communities, and technology-forming companies can help better to create a safe online ecosystem. There is a need to invest in future studies exploring advanced techniques to support and enhance communication means in youth exploiting positive and safe online experiences.

REFERENCES

- [1] M. Mihajlov and L. Vejmelka, "Internet addiction: a review of the first twenty years," *Psychiatria Danubina*, vol. 3, pp. 260–272, 2017.
- [2] E. Englander, "Risky business talking with your patients about cyberbullying and sexting," *Child and Adolescent Psychiatric Clinics of North America*, vol. 27, pp. 287–305, 2018.
- [3] V. Carli, "A newly identified group of adolescents at 'invisible' risk for psychopathology and suicidal behavior: findings from SEYLE study," *World Psychiatry*, vol. 13, pp. 78–86, 2014.
- [4] M. E. P. Seligman and J. Tierney, "We aren't built to live in the moment," *New York Times*, 2018.
- [5] S. S. A. Guan and K. Subrahmanyam, "Youth internet use: risks and opportunities," *Current Opinion in Psychiatry*, vol. 22, pp. 351–356, 2009.
- [6] M. A. Moreno, L. Jelenchick, E. Cox, et al., "Problematic Internet use among US youth: a systematic review," *Archives of Pediatrics and Adolescent Medicine*, vol. 165, no. 9, pp. 797–805, 2011.
- [7] M. A. Moreno, L. Jelenchick, R. Koff, J. Eikoff, C. Diermyer, and D. A. Christakis, "Internet use and multitasking among older adolescents: an experience sampling approach," *Computational Human Behavior*, vol. 28, no. 4, pp. 1097–1102, 2012.
- [8] E. L. Anderson, E. Steen, and V. Stavropoulos, "Internet use and problematic Internet use: a systematic review of longitudinal research trends in adolescence and emergent adulthood," *International Journal of Adolescent Youth*, vol. 22, no. 4, pp. 430–454, 2017.

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

- [9] M. K. LeBourgeois et al., "Digital media and sleep in childhood and adolescence," *Pediatrics*, vol. 140, Suppl. 2, pp. S92–S96, 2017.
- [10] T. N. Robinson, J. A. Banda, L. Hale, A. S. Lu, F. Fleming-Milici, S. L. Calvert, and E. Wartella, "Screen media exposure and obesity in children and adolescents," *Pediatrics*, vol. 140, Suppl. 2, pp. S97–101, 2017.
- [11] L. A. Jelenchick, J. Eickhoff, D. A. Christakis et al., "The problematic and risky Internet use screening scale (PRIUSS) for adolescents and young adults: scale development and refinement," *Computational Human Behavior*, vol. 35, 2014.
- [12] L. A. Jelenchick, J. Eickhoff, C. Zhang, K. Kraninger, D. A. Christakis, and M. A. Moreno, "Screening for adolescent problematic internet use: validation of the problematic and risky internet use screening scale (PRIUSS)," *Academics Pediatrics*, vol. 15, no. 6, pp. 658–665, 2015.
- [13] M. A. Moreno, A. Arseniev-Koehler, and E. Selkie, "Development and testing of a 3-item screening tool for problematic Internet use," *Journal of Pediatrics*, vol. 176, pp. 167–172, 2016.
- [14] A. Mayhew and P. Weigle, "Media engagement and identity formation among minority youth," *Child and Adolescent Psychiatric Clinics of North America*, vol. 27, pp. 269–285, 2018.
- [20] D. M. Hilty, "Advancing science, clinical care and education: shall we update Engel's biopsychosocial model to a bio-psycho-socio-cultural model?" *Psychology and Cognitive Science*, vol. 1, no. 1, pp. 25–39, 2016.
- [21] D. Bavelier, C. S. Green, and M. W. G. Dye, "Children, wired – for better and for worse," *Neuron*, vol. 67, no. 5, pp. 692–701, 2010.
- [22] M. Drouin, K. N. Vogel, A. Surbey, et al., "Let's talk about sexting, baby: computer-mediated sexual behaviors among young adults," *Computational Human Behavior*, vol. 29, no. 5, pp. 25–30, 2012.
- [23] E. M. Selkie, J. A. Fales, and M. A. Moreno, "Cyberbullying prevalence among United States middle and high school aged adolescents: a systematic review and quality assessment," *Journal of Adolescent Health*, vol. 58, no. 2, pp. 125–133, 2016.
- [24] T. Anderson, "Identifying Signs of Excessive Internet Use," *Journal of Education Technology*, vol. 15, no. 2, pp. 150–162, 2022.
- [25] R. Ahmed, "Cyberbullying in Pakistan: Understanding the Victims' Perspective," *Journal of Digital Culture*, vol. 15, no. 3, pp. 45–56, 2020.
- [26] S. Ali, "Reporting Mechanisms for Cyberbullying in Pakistan," *Cyberlaw Revolution*, vol. 12, no. 2, pp. 78–89, 2020.
- [27] C. A. Anderson and K. E. Dill, "Video games and aggressive thoughts, feelings, and behavior in the laboratory and in life," *Journal of Personality and Social Psychology*, vol. 78, no. 4, pp. 772–790, 2000.
- [28] H. Aziz, "Impact of Excessive Online Activity on Academic Performance," *Educational Insights*, vol. 8, no. 4, pp. 150–162, 2020.
- [29] M. Bashir, "Health Implications of Prolonged Screen Time," *Health Journal of Pakistan*, vol. 23, no. 1, pp. 33–45, 2020.
- [30] J. Billieux, L. Rochat, G. Ceschi, P. Carraze, and M. Van der Linden, "Validation of a short French version of the Internet Addiction

- Test,” *Computatioanl Human Behavior*, vol. 29, no. 3, pp. 175–182, 2015.
- [31] E. S. Bordin, “The generalizability of the psychoanalytic concept of working alliance,” *Psychotherapy Theory Research Practice*, vol. 16, no. 3, pp. 252–260, 1979.
- [32] L. Brown, “Initiating Conversations about Internet Habits,” *Education Today*, vol. 8, no. 4, pp. 45–56, 2019.
- [33] S. E. Caplan, “Relations among loneliness, social anxiety, and problematic Internet use,” *CyberPsychology Behavior*, vol. 10, no. 2, pp. 234–242, 2007.
- [34] W. Chen and Y. Peng, “Online social support: A theoretical perspective,” *Computational Human Behavior*, vol. 24, no. 1, pp. 258–270, 2008.
- [35] M. Clark, “Developing Individualized Treatment Plans,” *Clinical Psychology Revolution*, vol. 18, no. 3, pp. 33–45, 2021.
- [36] R. Davis, “Evaluating Mental and Physical Health Impact of Excessive Internet Use,” *Jouranl of Behavior Studies*, vol. 11, no. 3, pp. 89–101, 2020.
- [37] J. Evans, “Integrating Digital Literacy into the Curriculum,” *Educational Insights*, vol. 7, no. 2, pp. 100–112, 2022.
- [38] A. Farooq, “Support Services for Cyberbullying Victims,” *Jouranl of Behavior Studies*, vol. 10, no. 2, pp. 65–77, 2018.
- [39] K. Harris, “Discussing Risks Associated with Excessive Internet Use,” *Journal of Mental Health*, vol. 29, no. 1, pp. 40–52, 2020.
- [40] N. Hassan, “Mental Health Stigma in Pakistani Culture,” *The Journal of Social Psychology*, vol. 19, no. 3, pp. 99–110, 2020.
- [41] S. Haugh and L. Rutter, “The importance of confidentiality in psychotherapy,” *Journal of Behavior Studies*, vol. 21, no. 7, pp. 12–15, 2010.
- [42] M. A. Hubble, B. L. Duncan, and S. D. Miller, “The Heart and Soul of Change: What Works in Therapy”. *American Psychological Association*, 1999.
- [43] F. Hussain, “Strengthening Cybercrime Laws in Pakistan,” *The Journal of Social Psychology.*, vol. 14, no. 2, pp. 115–127, 2022.
- [44] S. Iqbal, “Social Media Addiction Among Youth,” *Journal of Behavior Studies*, vol. 11, no. 3, pp. 189–200, 2021.
- [45] P. Johnson, “Building Rapport with Patients and Students,” *Health Journal of Pakistan*, vol. 23, no. 1, pp. 33–45, 2021.
- [46] R. Khalid, “Healthy Online Habits for Youth,” *Digital Well-being Magazine*, vol. 7, no. 2, pp. 45–56, 2019.
- [47] A. Khan and S. Rehman, “Educational Programs on Cyberbullying,” *Education Today*, vol. 15, no. 1, pp. 23–35, 2019.
- [48] D. M. Kivlighan and P. Shaughnessy, “The relationship between therapeutic alliance and outcome: A meta-analysis,” *Journal of Counseling Psychology*, vol. 47, no. 3, pp. 288–298, 2000.
- [49] D. J. Kuss and M. D. Griffiths, “Internet gaming addiction: A systematic review of empirical research,” *International Journal of Mental Health and Addiction*, vol. 10, no. 2, pp. 278–296, 2012.
- [50] A. Lee, “Conducting Thorough Assessments Using Standardized Tools,” *Cyberlaw Review*, vol. 12, no.

Role of Parent-Adolescent Communication to Prevent Cyberbullying in Youth: Challenges and Opportunities

- 2, pp. 78-89, 2021.
- [51] D. Lewis, "Offering Counseling and Support Groups for Internet Use," *Counseling Today*, vol. 10, no. 2, pp. 65-77, 2020.
- [52] Z. Malik, "Mental Health Services Accessibility in Pakistan," *Health Services Journal*, vol. 18, no. 2, pp. 100-112, 2020.
- [53] F. Martin, "Providing Information on Healthy Internet Use," *Digital Well-being Magazine*, vol. 7, no. 2, pp. 45-56, 2021.
- [54] J. McLeod, *An Introduction to Counseling*. McGraw-Hill Education, pp. 23-31, 2013.
- [55] S. Moore, "Implementing School-wide Programs for Digital Well-being," *Public Health Journal*, vol. 22, no. 4, pp. 102-115, 2020.
- [56] R. Naseer, "Improving Counseling Accessibility," *Journal of Mental Health*, vol. 29, no. 1, pp. 40-52, 2022.
- [57] M. Nawaz, "Balancing Screen Time for Better Academic Performance," *Academic Review*, vol. 16, no. 3, pp. 78-89, 2021.
- [58] J. C. Norcross, *Psychotherapy Relationships That Work: Evidence-Based Responsiveness*. Oxford University Press, 2011.
- [59] J. C. Norcross and B. E. Wampold, "Evidence-based therapy relationships: The 'what works' and 'how' of therapy," *Journal of Clinical Psychology*, vol. 67, no. 1, pp. 1-9, 2011.
- [60] K. J. Prager, *The Therapeutic Alliance: A Research-Based Guide*. Routledge, 2018.
- [61] B. A. Primack, A. Shensa, J. E. Sidani, et al., "Social media use and perceived social isolation among young adults in the U.S.," *American Journal of Preventive Medicine*, vol. 53, no. 1, pp. 1-8, 2017.
- [62] T. Raza, "Awareness Campaigns Against High-Risk Behaviors," *Public Health Journal*, vol. 22, no. 4, pp. 102-115, 2021.
- [63] C. R. Rogers, *On Becoming a Person: A Therapist's View of Psychotherapy*. Houghton Mifflin, 1961.
- [64] L. Sadiq, "Cultural Taboos and Mental Health in Pakistan," *Culture and Society*, vol. 10, no. 3, pp. 55-67, 2019.
- [65] L. Scott, "Collaborating with Parents and Guardians," *Academic Review*, vol. 16, no. 3, pp. 78-89, 2021.
- [66] U. Shahid, "Enforcement of Cybercrime Laws in Pakistan," *Cybersecurity Today*, vol. 13, no. 2, pp. 89-101, 2021.
- [67] A. Shensa, J. E. Sidani, B. A. Primack, et al., "Social media use and perceived social isolation among young adults in the U.S.," *American Journal of Preventive Medicine*, vol. 53, no. 1, pp. 1-8, 2017.
- [68] J. Smith, "Creating a Safe and Non-judgmental Environment," *Journal of Social Psychology*, vol. 19, no. 3, pp. 99-110, 2020.
- [69] S. Sue, J. K. Y. Cheng, C. S. Saad, and J. Cheng, "Asian American mental health: A cultural and contextual perspective," *American Psychologist*, vol. 67, no. 7, pp. 532-544, 2012.
- [70] M. Taylor, "Monitoring Academic Performance and Social Interactions," *Health Services Journal*, vol. 18, no. 2, pp. 100-112, 2021.
- [71] R. J. J. M. van den Eijnden, G. J. Meerkerk, A. A. Vermulst, et al., "The social media disorder scale: Validity and reliability," *Computers in Human Behavior*, vol. 61, pp. 278-285, 2016.
- [72] R. Walker, "Using Surveys and

- Questionnaires for Assessment,” *Culture and Society*, vol. 10, no. 3, pp. 55-67, 2019.
- [73] K. White, “Promoting Awareness about Balanced Lifestyle,” *Wellness and Health*, vol. 8, no. 2, pp. 45-58, 2019.
- [74] F. Yasin, “Digital Detox Programs for Youth,” *Wellness and Health*, vol. 8, no. 2, pp. 45-58, 2021.
- [75] K. S. Young, “Internet addiction: The emergence of a new clinical disorder,” *CyberPsychology & Behavior*, vol. 1, no. 3, pp. 237-244, 1998.
- [76] L. Zielinski and M. Murakami, “Family involvement in adolescent treatment: The role of parents,” *Journal of Family Psychology*, vol. 34, no. 5, pp. 589-598, 2020.
- [77] R. M. Cassidy, F. Yang, F. Kapczinski, and I. C. Passos, “Risk factors for suicidality in patients with schizophrenia: A systematic review, meta-analysis, and meta-regression of 96 studies,” *Schizophrenia Bulletin*, vol. 44, no. 4, pp. 787-797, 2018.
- [78] S. Paul, P. K. Smith, and H. H. Blumberg, “Investigating legal aspects of cyberbullying,” *Psicothema*, vol. 24, no. 4, pp. 640-645, 2012.
- [79] C. P. Barlett and M. Fennel, “Examining the relation between parental ignorance and youths’ cyberbullying perpetration,” *Psychology of Popular Media Culture*, vol. 7, no. 4, pp. 547-560, 2018.
- [80] T. M. O’Connor, M. Hingle, R. J. Chuang, T. Gorely, T. Hinkley, R. Jago, J. Lanigan, N. Pearson, and D. A. Thompson, “Conceptual understanding of screen media parenting: Report of a working group,” *Childhood Obesity*, vol. 9, no. 1, pp. 110-118, 2013.
- [81] H. E. Lee, J. Y. Kim, and C. Kim, “The Influence of Parent Media Use, Parent Attitude on Media, and Parenting Style on Children’s Media Use,” *Children*, vol. 9, no. 1, p. 37, 2022.
- [82] L. M. Padilla-Walker and S. M. Coyne, “Turn that thing off! Parent and adolescent predictors of proactive media monitoring,” *Journal of Adolescence*, vol. 34, pp. 705-715, 2011.
- [83] K. Fousiani, P. Dimitropoulou, M. P. Michaelides, and S. Van Petegem, “Perceived Parenting and Adolescent Cyber-Bullying: Examining the Intervening Role of Autonomy and Relatedness Need Satisfaction, Empathic Concern and Recognition of Humanness,” *Journal of Child and Family Studies*, vol. 25, pp. 2120-2129, 2016.
- [84] P. Greenfield and Z. Yan, “Children, adolescents, and the Internet: A new field of inquiry in developmental psychology,” *Developmental Psychology*, vol. 42, no. 3, pp. 391-394, 2006.
- [85] M. A. Zimmerman and S. Warschausky, “Empowerment theory for rehabilitation research: Conceptual and methodological issues,” *Rehabilitation Psychology*, vol. 43, no. 1, pp. 3-16, 1998.



Enhanced Malware Detection Using Grey Wolf Optimization and Deep Belief Neural Networks

Zohaib Ahmad¹, Obaidullah², Muhammad Ammar Ashraf³ and Muhammad Tufail⁴

¹Faculty of Electronics and Information Engineering, Beijing University of Technology, Beijing, China.

²Department of Computer Science, University of Alabama at Birmingham AL 35205, USA.

³Department of Computer Science, Ripah international University, Sahiwal Campus, Sahiwal, Pakistan

⁴Department of Computer Science, Government Postgraduate College, Nowshera, KP, Pakistan

Correspondence Author: ahmedzohaib03@gmail.com

Received: Aug 03, 2024; **Accepted:** Aug 19, 2024; **Published:** Sep 12, 2024

ABSTRACT

Standard identification methods are flatter and less effective as attacks from malware get increasingly sophisticated. Considering current malware outbreaks employ tactics such as polymorphism, obfuscation and encryption, to avert identification, growing complicated approaches must be developed. This paper deals with a mixed model utilizing Deep Belief Neural Network (DBNN) for classifying and Grey Wolf Optimization (GWO) for choosing features. Whereas DBNN encodes complicated patterns by hierarchical learning, GWO optimizes the choosing of the more essential features, lowering the cost of computing and dataset complexity. Investigations reveal that the suggested GWO-DBNN model beats existing machine learning procedures in

terms of detection accuracy, recall, precision, and false positive rate (FPR). These mixed tactics offer dependable and scalable solutions to the challenges faced by modern malware threats.

Keywords: Deep neural networks, DNNs, Malware analysis, Feature Engineering, Metaheuristic algorithms

1. INTRODUCTION

Malware, shorthand for "harmful software," is one of the largest and most major risks to broad cybersecurity nowadays. This word covers a wide range of hazardous software forms, spanning viruses, worms, ransomware, spyware, and others. Malware attacks have risen dramatically in the past few years, owing to the expansion of correlated networks, the rise of cloud computing, and the rapidly evolving digital world [1]. Typically, the identification of malware relies on signature-based platforms which match established signatures for recognizing potential dangers [2]. While such devices have been useful in the past, they endure considerable constraints especially whenever it comes to identifying zero-day attacks [3].

According to authors [4], innovative methods of evasion involving polymorphism are employed by contemporary malware creators for allowing their harmful software to alter its code architecture without losing its ability to trigger harm. Also, methods of obfuscation make it more challenging for ordinary antivirus programs to identify hazardous

behavior by hiding the real code from monitoring systems [5]. According to authors [6], these approaches greatly reduce the efficacy of static signature-based identification, forcing the use of more dynamic strategies that might evolve with these dynamic challenges. According to the authors [7] with the quick augmentation in the variation of malware methods, ML and DL have developed into acute tools in advocate the identification of malware. These approaches can cultivate behaviors and patterns from historical data, clearing them to recognize known and evolving malware whereas depending on prearranged signature. According to the authors, ML methods [8] containing Naïve Bayes, Support Vector Machines (SVM), and Random Forests may rationalize classifying via examination of dynamic and static features.

The authors [1] describe the typical machine learning approaches could have trouble with highly dimensional raw data, which might contain unimportant or replicate features. According to [6][17], over fitting is possible if models operate effectively with data used for training but harshly on data that is not known. Besides, dataset with high dimensions augments the computing cost, execution it

unfitting for real-time revealing of viruses. The authors [2] described competent selection of features is vivacious to lowering redundancy and keeping valued properties for categorization

This research presents an optimized architecture incorporating GWO for picking features with DBNN for classifying. [6] Devised GWO, a metaheuristic algorithm inspired by grey wolf social structures and hunt tactics that can quickly traverse huge searching areas and select finest subset of attributes. The authors [5] discovered that GWO successfully decreases the complexity of challenging malware samples. DBNN are an unsupervised neural network architecture made consisting of layers of Restricted Boltzmann Machine. DBNNs can acquire hierarchical structures from vast data sets while enhancing the accuracy of classification by automatically recognizing complex connections among characteristics [8] [9].

Main Contributions

1. This paper leads an optimized structure that incorporates GWO for the selection of the features with DBNN for malware classifying tasks. The utilization of GWO advances feature collection by competently decreasing the size of the data samples, guaranteeing that only the best appropriate features are employed, subsequently augmenting classification enactment and

sinking computational burden.

2. By engaging GWO, the suggested methodology effectually addresses the tasks impersonated by high-dimensional data samples, which frequently cover irrelevant or redundant features. This effects in a reduction of overfitting and advances the generality of the model, constructing it more appropriate for actual malware revealing.
3. By utilizing DBNN, the framework may automatically recognise hierarchy relationships in malware knowledge, boosting its ability to recognize malware variations that have been identified and those which are unknown. When contrasted with typical machine learning methods, the architecture of deep learning delivers superior accuracy in classification since it can deal with complicated feature interactions more effectively.
4. The hybrid GWO-DBNN structure delivers an accessible result for dynamic and real-time malware revealing, capable of adjusting to embryonic malware dangers such as obfuscated and polymorphic malware. This creates the model appropriate for disposition in modern cybersecurity situations where fast and adaptive detection is critical.

The remainder of the paper is organized as: Section 2 deliberates related work, Section 3 introduces our metaheuristic algorithm and deep-learning technique

to malware detection classification, and Section 4 evaluates its performance in comparison to existing malware detection. Section 5 takes the paper to its conclusion.

2. LITERATURE REVIEW

2.1. Machine Learning and Malware Detection

In the domain of malware detection, there are primarily two types of analysis: static analysis and dynamic analysis. Static analysis involves extracting features from the malware code without executing it. Commonly extracted features include opcode sequences, bytecode frequencies, and control flow graphs[1]. Naïve Bayes and Decision Trees were among the earliest machine learning (ML) models used in static analysis. For example, the authors pioneered the use of Naïve Bayes to classify malware based on binary byte sequences, which represented a breakthrough in automated malware detection. While static examination has been highly successful, current malware frequently uses code obfuscation and polymorphism methodologies, causing static approaches fewer effective since malware could alter its appearance while still expressing hazardous behaviors.

Dynamic analysis, on the other hand, implements malware in a controlled environment (for example a sandbox), consenting its behavior to be monitored in the real time. This tactic records runtime behavior, containing network activity and system calls and, making it difficult for malware to evade detection. ML processes such as SVM

are used in dynamic study to classify malware based on behavioral characteristics. SVM has had some success in dynamic analysis, but it struggles when dealing with huge amounts of data samples.

Despite these advances, traditional machine learning models still struggle with high-dimensional data—datasets that include numerous irrelevant or redundant features. Such data can lead to overfitting, where the model performs well on training data but poorly on unseen data [7][10]. Besides, high-dimensional data samples upsurges the computational difficulty of the models, restraining their applicability in real-time malware revealing scenarios. Consequently, real feature variety is crucial in augmenting the enactment of ML models for malware revealing by decreasing irrelevant data while stabilizing the most informative features.

2.2. Feature Selection Technique

Feature selection plays a critical role in improving the performance of machine learning models, particularly when dealing with large, high-dimensional datasets such as those used in malware detection. Feature selection helps reduce the dataset size, making the model more efficient by eliminating irrelevant and redundant features. Traditional filter-based methods such as Chi-square and Information Gain evaluate the significance of each feature independently of the classification algorithm. While these methods are computationally efficient, they often fail to capture complex interactions between features, which is essential in

malware datasets.

To address these limitations, researchers easily adopted metaheuristic algorithms such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO) for feature selection [7]. These algorithms are for searching high-dimensional feature spaces, as they balance exploration (searching through the solution space) and exploitation (refining the best solutions found) during the feature selection process. However, each method has its drawbacks. For example, PSO is prone to slow convergence, while ACO can have high computational overhead.

In [6] the authors stated the GWO procedure that was recognized as an effective choice for highly dimensional feature selection challenges. Motivated by the hunting behavior and social structure of grey wolves in the natural world, GWO classifies them as alpha, beta, and delta wolves, with alpha wolves being the most beneficial solution. The technique optimizes exploitation and exploration by altering the wolf's location concerning the most suitable feature set, allowing for rapid and effective convergence. It makes GWO exceptionally excellent for processing huge, complicated data sets, such as those encountered in detecting malware.

2.3. Deep Learning in Malware Classification

Deep Learning (DL) models have been transformative in the field of malware detection, particularly in handling high-dimensional data. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Deep

Neural Networks (DNNs) have been employed to automatically extract and learn patterns from large malware datasets. DL models offer the advantage of learning hierarchical features, which allows them to generalize better than traditional machine-learning methods that rely on manual feature extraction.

DBNNs are distinguished from other deep learning models by their capacity to grip complicated data samples like those used in malware classification. DBNNs are constructed up of many layers of Restricted Boltzmann Machines (RBMs), which are unsupervised learning processes. RBMs aim to acquire a probabilistic representation of the input data by minimizing the variations between the real input and the rebuilt output. After initial training on RBMs, refine the DBNN with backpropagation to optimize the system for classifications. The structural design of DBNNs marks them as compatible with discovering sophisticated malware, for example, they are accomplished by learning multiple stages of abstraction from raw input features. This facility to model deep non-linear relations between features tolerates DBNNs to classify complex malware designs that may be neglected by typical ML models. In this examination, the combination of GWO for feature assortment and DBNNs for classification is offered to optimize the accuracy of the feature selection and classification in malware revealing.

3. METHODOLOGY

3.1. Data Preprocessing

The processing of data is an essential phase in prepping the dataset for use in

training and classifications. The actual malware datasets utilized in the present research were derived from the Microsoft Malware Classification Challenge [9] on Kaggle. This collection includes more than 10,000 samples from numerous malware families, among them Ramnit, Simda, Kelihos, and Vundo. The dataset covers the static and dynamic information, such as system call traces and opcode frequency, making it suitable for both static and dynamic training. Preprocessing encompasses numerous stages:

- Missing values can have a serious influence on the model's efficiency. In this research, the missing data has been solved via mean imputation for numerical parameters and median imputation for categorical characteristics.
- Normalization applies Min-Max scaling to align every value of the feature across 0 and 1. This guarantees that characteristics with wide ranges do not have an excessive effect on the learning process.
- For categorical features, such as malware families, one-hot encoding is used to convert categorical values into binary vectors. This avoids any ordinal interpretation of categorical variables, ensuring that the model does not infer unnecessary relationships between malware families.
- The dataset is divided into train (80%) and test (20%) batches for evaluating the efficacy of the

model that was suggested. Five-fold cross-validation is implemented to verify stability while avoiding overfitting.

3.2. Feature Selection using Grey Wolf Optimization (GWO)

The procedure called GWO [11] [12] is a metaheuristic approach influenced by grey wolves' natural hunting techniques and leadership framework. GWO organizes wolves into four categories: alpha, beta, delta, and omega. The alpha wolf reveals the optimum respond (optimal feature subset), whilst the beta and delta wolves direct the search process.

The GWO method estimates the distance that exists among the wolves and their prey and repeatedly updates their locations to arrive at the optimal response. The location of updates are determined using the following formula as:

$$D_{\alpha} = |C_1 \cdot X_{\alpha}(t) - X(t)| \quad (1)$$

X_{α} provides the alpha wolf's position, while D_{α} provides the distance from the optimal feature subset. The technique repeatedly alters the wolves' placements to reduce the space of features and pick the most appropriate subset for categorization.

3.3. Classification Using Deep Belief Neural Networks (DBNN)

The architecture of DBNN is shown in figure 1. After identifying the appropriate feature subset with GWO, DBNN employs it for identifying malware. DBNNs are made up of numerous layers of Restricted Boltzmann Machines (RBMs) that are unsupervised learning models [13][14]. RBM learns to rebuild input by retaining the statistical connections

among hidden and visible units [15].

The weight adjustment for every RBM follows a certain rule is

$$\Delta W_{ij} = \eta (< V_i h_j >_{data} - (< V_i h_j >_{recon})) \quad (2)$$

Where h_j is the hidden unit, V_i designates the visible unit, and η

represents the learning rate. After pretraining with RBMs, the DBNN is fine-tuned using backpropagation method to classify malware as either malicious or benign based on the optimized feature subset. The flow diagram of the whole methodology has been shown in figure 2

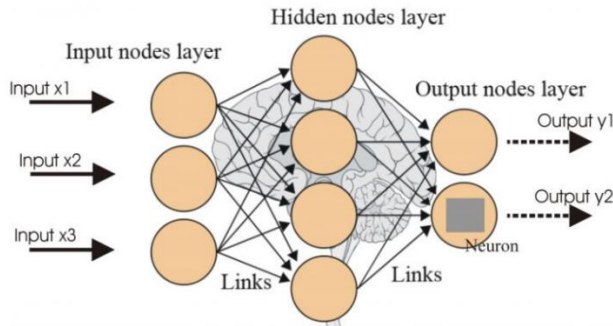


Figure 1: Architecture of DBNN

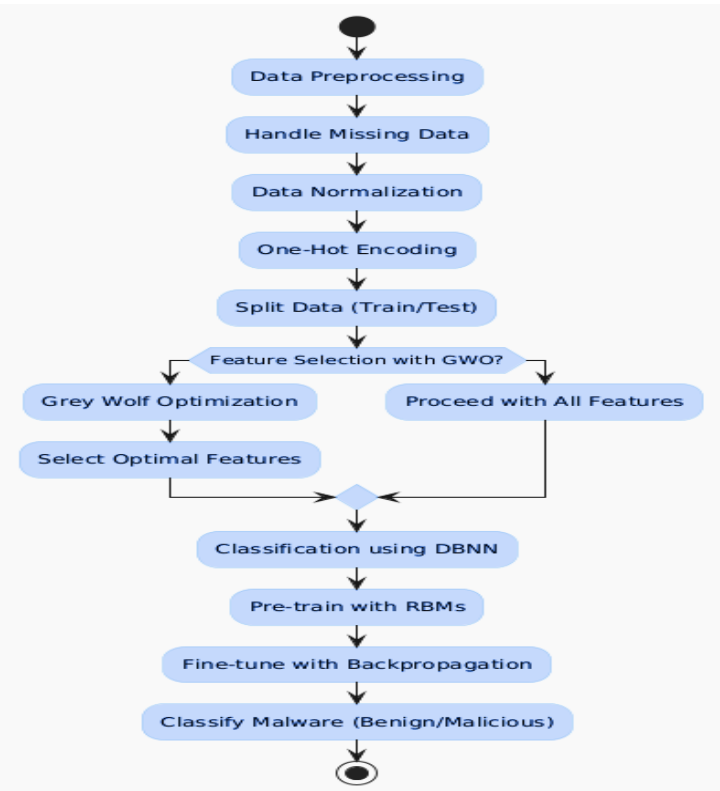


Figure 2: Flow Diagram of the proposed GWO-DBNN Malware Detection

4. RESULTS

The proposed GWO-DBNN model was evaluated using key performance metrics such as accuracy, precision, recall, F1-score, and false positive rate (FPR). The results were compared against traditional machine learning models like SVM, Naïve Bayes, and Decision Trees.

4.1. Performance Metrics

To assess the efficacy of the GWO-DBNN model, the following performance metrics have been employed:

- Accuracy: Evaluate the proportion of correctly classified instances amid the total instances.
- Recall: Replicates the proportion of true positive detections mid all actual positive instances.
- Precision: Designates the proportion of true positive detections between all positive predictions.
- F1-Score: The harmonic means of recall and precision, providing a balance between the two.
- FPR: The rate at which benign samples are incorrectly categorized as malicious.

4.2. Quantitative Results

The table below summarizes the performance of the GWO-DBNN model compared to traditional ML models on the malware detection task: From the Figure 3, it is cleared that

proposed **GWO-DBNN** model consistently outperformed traditional ML models across all metrics, particularly in terms of reducing false positives and improving overall accuracy.

Table 1: Performance Comparison

Model	Accuracy	Recall	Precision	F1-score	FPR
SVM	91.50%	90.8%	90.0%	89.40%	3.0%
Decision Tree	89.70%	87.40%	88.90%	87.80%	3.4%
Nave Bayes	88.20%	86.50%	86.40%	85.70%	4.0%
GWO-DBNN	95.80%	93.8%	93.70%	94.10%	1.7%

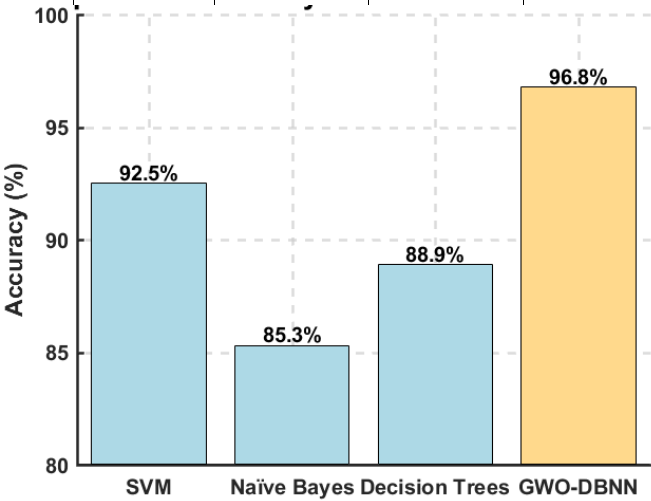


Figure 3: Comparative analysis of Malware Detection Model

5. DISCUSSION

The experimental findings show that the GWO-DBNN model improves malware identification and classification over standard ML

approaches [15]. By using GWO for feature selection, the model decreases the dataset's dimensionality, increasing computing efficiency and classification accuracy.

The inclusion of DBNN enhances the model's performance by enabling hierarchical feature learning, which

allows the network to automatically recognize complicated patterns in malware behavior. The combined use of GWO and DBNN has shown to be a viable technique for dealing with current malware issues such as obfuscation or zero-day attacks.

6. CONCLUSION

This article describes a unique hybrid system for identifying malware utilizing GWO for choosing features and DBNN for classifications. The suggested approach outperforms standard machine learning methods in terms of malware detection, precision, accuracy, and computing the economy at large.

Future work will focus on further optimizing the model, investigating other deep learning architectures, and increasing its application to other cybersecurity concerns such as ransomware and intrusion detection.

REFERENCES

- [1] M. G. Schultz, E. Eskin, F. Zadok, and S. J. Stolfo, "Data mining methods for detection of new malicious executables," *Proceedings of the IEEE Symposium on Security and Privacy*, vol. 2001, pp. 1-11, 2001.
- [2] K. Rieck, P. Trinius, C. Willems, and T. Holz, "Automatic analysis of malware behavior using machine learning," *Journal of Computer Security*, vol. 19, pp. 639-668, 2011.
- [3] H. S. Anderson and P. Roth, "Ember: An open dataset for training static PE malware machine learning models," *arXiv Preprint*, arXiv:1804.04637, pp. 1-12, 2018.
- [4] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and J. Blasco, "Dendroid: A text mining approach to analyzing and classifying code structures in Android malware families," *Expert Systems with Applications*, vol. 41, pp. 1104-1117, 2014.
- [5] X. Xu, H. Shen, and H. Chen, "Trafficav: An effective and explainable detection of mobile malware behavior using network traffic," *Proceedings of the 2016 IEEE/ACM International Symposium on Quality of Service*, pp. 1-10, 2016.
- [6] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," *Advances in Engineering Software*, vol. 69, pp. 46-61, 2014.
- [7] Y. Ye, D. Wang, T. Li, and D. Ye, "An intelligent PE-malware detection system based on association mining," *Journal of Computer Virology*, vol. 4, pp. 323-334, 2008.
- [8] Y. Bengio, "Learning deep architectures for AI," *Foundations and Trends in Machine Learning*, vol. 2, pp. 1-127, 2009.
- [9] Z. Ahmad, M. S. Pathan, and A. Wajahat, "A comparative analysis of malware detection methods: Traditional vs. machine learning," *International Journal for Electronic Crime Investigation*, vol. 7, pp. 3-18, 2023.
- [10] R. Ahmad, H. Salahuddin, A. U. Rehman, A. Rehman, M. U. Shafiq, M. A. Tahir, and M. S. Afzal, "Enhancing database security through AI-based intrusion detection system," *Journal of Computing & Biomedical Informatics*, vol. 7, pp. 1-12, 2024.
- [11] H. Rezaei, O. Bozorg-Haddad, and X. Chu, "Grey wolf optimization (GWO) algorithm," in *Advanced Optimization by Nature-Inspired*

Algorithms, pp. 81-91, 2018.

[12] A. Bilal, A. Alzahrani, A. Almuhaimeed, A. H. Khan, Z. Ahmad, and H. Long, "Advanced CKD detection through optimized metaheuristic modeling in healthcare informatics," *Scientific Reports*, vol. 14, pp. 12601, 2024.

[13] R. Khan, N. Iltaf, M. U. Shafiq, and F. U. Rehman, "Metadata-based cross-domain recommender framework using neighborhood mapping," 2023 International Conference on Sustainable Technology and Engineering (i-COSTE), pp. 1-8, 2023.

[14] M. F. Chishti, M. Rao, M. W. Raffat, and S. Rafi, "Estimating corporate risk and corporate value: An application of Altman's Z-score on the KSE-30 index," *International Journal of Contemporary Issues in Social Sciences*, vol. 3, pp. 2833-2841, 2024.

[15] M. U. Shafiq and A. I. Butt, "Segmentation of brain MRI using U-Net: Innovations in medical image processing," *Journal of Computational Informatics & Business*, vol. 1, pp. 1-15, 2024.

[16] A. Ullah, M. Waqar, S. S. Nazir, A. Adnan, M. A. Khan, M. W. Raffat, and S. Rafi, "The impact of information communication technology and financial innovation on the financial performance of Chinese commercial banks," *Remittances Review*, vol. 9, pp. 364-383, 2024.

[17] M. Hamza, "Optimizing early detection of diabetes through retinal imaging: A comparative analysis of deep learning and machine learning algorithms," *Journal of Computational Informatics & Business*, vol. 1, no. 1, pp. 1-12, 2024.



**International Journal for
Electronic Crime Investigation**

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

DOI: <https://doi.org/10.54692/ijeci.2024.0803207>

Research Article

Vol. 8 issue 3 Jul-Sep 2024

Information Systems and Mechanism for Prevention of Cyber Frauds

Aftab Ahmad Malik¹, Waqar Azeem² and Mujtaba Asad³

¹ University of Kent, England

²Faculty of Computer Science, South Eastern Regional College, Down Patrick Ireland,
United Kingdom.

³Department of Automation and Control, Shanghai Jiao Tong University, Shanghai, China.

Corresponding author: dr_aftab_malik@yahoo.com

Received: Aug 05, 2024; **Accepted:** Aug 22, 2024; **Published:** Sep 12, 2024

ABSTRACT

Cyber criminals are targeting online frauds, exploiting anonymity to deceive. They use fake websites, fake ads and stolen credit or debit cards for purchases. Bank frauds, despite high-speed processing and technical assistance, can damage a bank's reputation and operational efficiency, necessitating a strong emphasis on business ethics in the banking sector. The machine learning and artificial intelligence enhance online security of information systems. US enforces anti-trust laws and promotes stakeholder rights, addressing fraud and identity theft through safety tips and civil law implementation. Cyber criminals steal personal information for unauthorized purchases, identity theft, and fraudulent activities. Machine learning and artificial intelligence can enhance online security and user awareness. AI-based threat detection analyzes network activity for cyberattacks, limiting damage. Multi-Factor Authentication (MFA) combines traditional passwords with biometric authentication for enhanced security. The application of Big Data systems allows administrations for the collection and analysis of Data and its storage obtained from various sources, using platforms like Hadoop, Apache Spark, and

Kafka for real-time processing and data analytics. Digital devices are increasingly being used in banking frauds, posing significant risks to both customers and the banking sector, necessitating stricter regulations and enforcement measures. Common banking sector issues include negligent, fraudulent, and deviant behavior, affecting various functions of getting, gathering, transporting, disbursing, loaning, trading, capitalizing, replacing, and servicing money-claims domestically and internationally. This paper discusses machine learning and anomaly detection techniques for preventing fraud in online payment systems, including behavioral profiling and Bagged Decision Tree models along with other methods.

Keywords: Cyber frauds, Information Systems, INFOSEC, Cyber Security, Financial services

1. INTRODUCTION

Fraud and white-collar crime in businesses and banking are increasing due to outdated technology. This research paper emphasizes the need for secure software and networks. Thieves use sophisticated software and technology to track and hack private information, using deceit and dishonesty to harm others. Employees often aid in scams, and legislation seems naive. Criminals flee due to secret identities, lack of evidence, poor investigation, and naive prosecution. This paper presents practical suggestions for safeguarding organizations' networks. Malik et al., [1] have discussed various aspects of frauds and fraudulent behavior.

Fraudulent activities involve securities marketing, hacking personal information, and stealing money. Law enforcement struggles, and research in accounting, society, and organizations is crucial for effective prevention and prosecution. Fraudulent activities involve securities marketing, hacking

personal information, and stealing money. Law enforcement struggles, and research in accounting, society, and organizations is crucial for effective prevention and prosecution. Over the past eight decades, white-collar crime research has evolved due to high-tech advancements and computer-related office changes, but few studies have explored cybercrime.

Cybercrime, a national threat, is more prevalent among younger criminals, with different trust signs. Banks aim to attract investors through stock market investments. It describes the methods to overcome White Collar Crimes in banking and other companies [2]. It emphasized on the use of digital devices in committing crime regarding Bank Frauds [3].

InfoSec refers to the strategies and methods used to safeguard sensitive business data from unauthorized access, modification, disruption, destruction, and inspection. An international standard is a globally recognized document developed by experts from various countries, containing rules, guidelines, and processes for consistent

outcomes. Three information security standards on International Standards include technical specifications. Major points of InfoSec are confidentiality, integrity, and availability, authenticity and non-repudiation. Authenticity in information security refers to the verification that data, transactions, communications, or documents are genuine. InfoSec emphasizes confidentiality, integrity, availability, authenticity, and non-repudiation, ensuring the authenticity of data, transactions, communications, or documents [4].

Information security standards outline documented processes for implementing, managing, and monitoring security controls, mitigating risk, and reducing vulnerabilities, while also ensuring regulatory compliance. Application security involves identifying and addressing vulnerabilities in web and mobile applications to prevent network breaches. Network security involves implementing policies to protect data and infrastructure, while cloud security involves off-site deployment strategies.

Meeting information standards is crucial for a company's best interest. It ensures regulatory compliance, prevents cyberattacks, and helps companies implement necessary measures, processes, policies, and controls. While compliance doesn't guarantee security, it serves as a starting point for companies to adapt to evolving cyber threats.

Financial Services Firms must register with FINRA, evaluating access management, branch controls, data loss prevention, employee training, incident response, risk assessment, supplier management, system change management, technical controls, and governance. Cybercrime and White-Collar Crime differ, with different tools used by hackers and fraudsters [4]. Banks must prioritize cybersecurity to protect against these threats. Government prioritizes cyber security to enhance national security, boost consumer confidence, and ensure system reliability. Each component must be individually considered to create an effective plan.

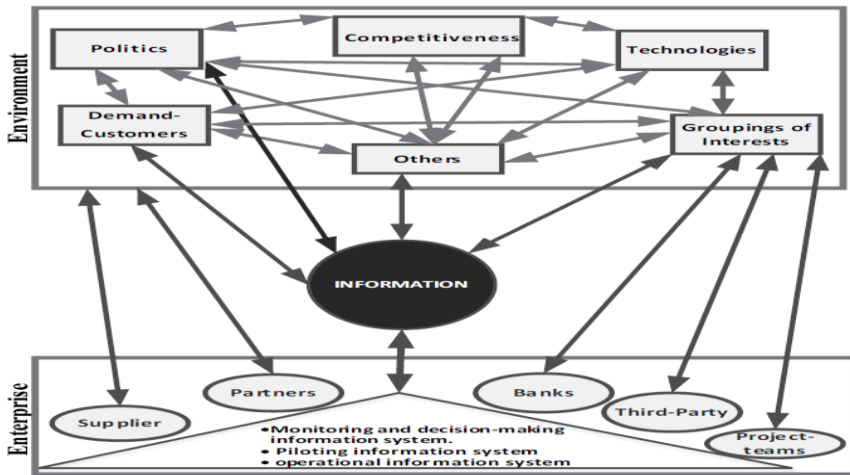


Figure 1: Modern Information System and I.T System

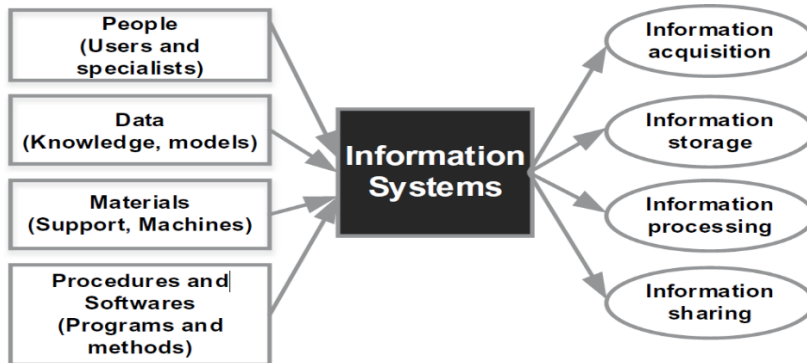


Figure 2: A systemic view of the company and the environment.

2. REVIEW OF LITERATURE

Malik et al., [1] discussed and proposed a comprehensive plan to combat Online Cyber frauds and suggested fraud

prevention Strategies. Malik et al., [2] have studied and the details of online cyber-crimes, specially, to fight with white-collar crimes occurring in Governmental organizations as well as

entrepreneurs and focused on the need for Strong Legislation and Ethics. Frauds in banks with the help of Electronic Devices and importance of “Business-Ethics” in the banking sector is important [3]. Anderson and Moore [5] has discussed in depth the online Cyber Crime and frauds and other matters related to Information Security have been presented with solutions. Rapid Action Battalion, discussed the matter about the financing of terrorism activities in the context of global perspective [6]. Enders and Sandler [7] has successfully deliberated on the effect of terrorism and its impact on the domestic economy of the affected country. The terrorist offences badly damage the financial markets and also the small business organizations. The groups behind terrorism financing need to be investigated and taken to task. Kshetri [8] and Vanini et al., [9] talk about the existence of online banking frauds, worldwide cybercrime Business, economic and planned standpoints. Table 1 presents a comprehensive overview of advanced

techniques being researched and implemented to combat online fraud in the financial and banking sectors.

2.1. Important Modern Information Systems

Key trends include AI and Machine Learning (ML) integration in analytics, blockchain technology for secure transactions, increasing data governance focus on GDPR, and server-less computing for flexibility and scalability. The structure of Information Systems (IS) has evolved significantly due to advancements in cloud computing, AI, data analytics, and cybersecurity. The new Information Systems (IS) are a sophisticated, modular, and cloud-driven architecture designed for large-scale data processing, business operations enhancement, and cybersecurity protection. In Table 1 below, we list currently developed methods applicable to Information Systems.

Table 1: Advance techniques to combat financial and banking frauds

Methods	
Online Payment Frauds	Encryption
Machine Learning	Anomaly Detection
Machine Learning	“Support Vector Machines (SVM)”
“Supervised and Unsupervised Learning Models”	“Recurrent Neural Networks (RNNs)”
Block-chain Method	Method of Multilayer perceptron (MLP)
Biometric Verification	Method of Random Forest and Gradient Boosting
Anti-Money Laundering (AML)	Emerging Trends in the Cyberber Crimes
Real-Time Fraud	Cryptocurrency related offences

GDPR compliance	Data mining Technique
-----------------	-----------------------

Modern IS architectures are more flexible, scalable, and integrated across various platforms and services. Key components include data analytics, security, and data analytics. Modern Information System's structures utilize IaaS, PaaS, and SaaS models for cost-effective, scalable infrastructure without heavy on-premise hardware, offering flexibility in data, applications, and virtualized environments.

Modern Information System structures also utilize IaaS, PaaS, and SaaS models for cost-effective, scalable infrastructure without heavy on-premise hardware, offering flexibility in data, applications, and virtualized environments. cost efficiency, scalability, and accessibility to cloud services, but also pose security and regulatory challenges. Storing data in the cloud offers cost efficiency, scalability, and accessibility, but also raises security risks and compliance challenges, particularly in sensitive industries [4].

Modern information systems prioritize distributed databases, storing data across physical or cloud environments, often using NoSQL and relational databases based on data complexity and requirements. The edge computing is gaining popularity for IoT applications, utilizing edge devices and cloud services. NoSQL databases like MongoDB and Cassandra are widely used for managing large-scale, unstructured data, offering flexibility, scalability, and efficient storage, particularly useful in big data applications.

Modern Information System structures prioritize security through advanced encryption, MFA, and zero-trust architectures, employing AI tools for breach detection and compliance with GDPR and privacy regulations. Big data analytics platforms like Apache Hadoop, Spark, and Kafka enable real-time and batch processing of diverse data sources, providing data visualization, predictive analytics, and business intelligence. The Hybrid and multi-cloud environments are being used by organizations for workload optimization, risk mitigation, and regulatory compliance, while collaboration and workflow systems like Microsoft Teams are integrated. Develops culture and pipelines are crucial for modern IS development, ensuring continuous system updates, testing, and deployment, with automation tools like Jenkins and Kubernetes playing critical roles.

3. ADVANCED METHODS TO COMBAT OFFENCES

Advanced technological and procedural strategies are being employed to combat online fraud and terrorist activities targeting banking and entrepreneurship. Financial institutions are utilizing (ML- Models) Machine Learning models for detection of doubtful and illegal transactions. preventing fraud by analyzing large datasets for unusual behaviors. Artificial Intelligence (AI) enhances Anti-Money Laundering and Counter-Financing of Terrorism efforts by

monitoring transactions, identifying threats, and enforcing regulatory compliance. Fraud detection systems use customer behavior data, like online activity patterns, to identify anomalies and abnormalities, forming profiles of normal user behavior to detect fraudulent actions. The hybrid models combine supervised learning for known cases and unsupervised methods to detect new types of fraud, ensuring system adaptation to evolving cybercriminal tactics.

The Payment fraud involves fraudulent or unauthorized transactions by cybercriminals, resulting in the loss of funds, personal property, interest, or sensitive information via the internet [9].

Ali et al., [10] reviewed the financial frauds detection, based on the technique of machine learning. Machine Learning techniques like SVM and ANN are of pivotal importance particularly when frauds are committed with credit; card fraud being the most common type. Meghana et al., [11] is another paper which explained the method of prediction of Financial Crime Using Machine Learning. Linear regression KNN algorithm, KNN algorithm and the K-nearest Neighbor (KNN) algorithm are the simple and early classification algorithms used for recommendation engines and image recognition. Supervised learning algorithms iteratively learn to predict target variables. Nasteski [12] provided an overview of the supervised machine learning methods.

“Threat Advice” offers industry-specific cybersecurity solutions and packages to protect organizations from

fraud detection and ensure the future of fraud prevention. Hassan et al [13] has proposed a valuable method for Fraud Detection in IoT-Based Financial Transactions Using “Anomaly Detection Techniques”. Online banking security is compromised due to vulnerable authentication schemes, allowing intruders to masquerade as legitimate users for unauthorized access Kiyani et al., [14].

No doubt Machine Learning has revolutionized data processing, enabling real-time, intelligent systems, particularly in fraud detection. Financial institutions invest in improving algorithms and data analysis technologies for accuracy. Abakarim et al., [15] has proposed a workable model in real time for the protection of frauds occurring regarding credit cards and an effective and efficient method indeed.

Block chain technology enhances security by providing transparency and immutability, making it harder for malicious actors to hide their activities across decentralized networks. Nowadays, the financial institutions are increasingly utilizing Multi-Factor Authentication (MFA) methods like facial recognition and fingerprint scanning to safeguard online accounts from unauthorized access. The regulations such as GDPR (General Data Protection Regulation) directives enforce strict standards for customer data handling, reducing fraud risk in the financial sector. They provide insights into advanced technologies for combating online threats. Malik et al., [1] have discussed various aspects of frauds and fraudulent behavior.

GDPR in banking mandates banks to

obtain explicit consent for data processing and marketing activities, ensuring it is free, specific, informed, and unambiguous. Baker [16] presented on impact of the GDPR: General Data Protection Regulation in banking.

Tanaka et al., [17] in their paper have discussed the “Gordon-Loeb-Model”, a crucial economics-based approach for organizations to determine the appropriate investment in cybersecurity-related activities. They further elaborated for facilitating malicious attacks. He has proposed empirical analysis on the issue of e-local governance. Gordon-Loeb Model is a crucial economics-based approach for organizations to determine appropriate investment in cybersecurity-related activities.

The Internet of Things (IoT) connects physical and virtual objects, enabling communication, data exchange, and personalization, but also poses a security risk due to increasing device numbers.

Altulaihan et al., [18] has published a useful paper regarding cybersecurity threats and discussed in detail about the countermeasures with justification all the techniques on the IoT. Zhu [19] in his valuable research paper uses Support Vector Machines for unsupervised financial data classification, combining histograms with Light GBM to fuse data from multiple sources for accurate company financial assessment.

Almazroi and Ayub [20] has introduced an applicable technique termed as “ResNeXt-embedded Gated-Recurrent-Unit model” which efficiently

addresses financial fraud in real-time and financial transaction processing, enhancing security and efficiency in the environment of wireless communications.

Mubarek and Adali [21] have discussed fraud detection in financial sectors, utilizing “machine-learning-algorithms” like Decision Trees and Naive Bayes to anticipate and quickly detect fraud. In the paper Kumar et al., [22] have highlighted and discussed the real-world credit-card fraud detection using Random Forest Algorithm (RFA), a “supervised-learning-algorithm”, which achieves 90% accuracy in detecting fraudulent transactions, both online and offline.

Banks are vulnerable to frauds, contributing to economic development. The study presented in Sood and Bhushan [23] explores bank fraud literature from 2000-2019, identifying major themes like regulatory and compliance-based studies and socio-psychological aspects. It is advised that future research should focus on customer vigilance and coping mechanisms. Teichmann and Falker [24] highlights the cryptocurrencies' role in financial crime, including money laundering and corruption, and proposes a more effective international regulation standard using Liechtenstein Blockchain as a benchmark. The research of Carneiro et al [25] discusses the development and deployment of a fraud detection system in an e-tail merchant, comparing “Machine Learning Methods” and manual classification, resulting in improved performance.

4. CONCLUSION

Banks and companies must establish a code of conduct, while adhering to the banking law, regulations, and international conventions. Trust companies and financial enterprises engage in illegal and unethical practices, such as money transfers, collection, exchanges, stock transfer services, and travel agents. There must be a strict check by the chief Executive. Commanding respect is very important due to reputation. Central banks manage money supply, influence monetary movement, and financial policy, becoming popular and trustworthy due to their reputation and measures. Incorrect trade-data is intentionally manipulated by businessmen to deceive and harm counterparts, causing damage to industry indices, business conditions, and investment opportunities. There must be a strict check by the chief Executive. Spiritual, political, and social values influence business ethics, impacting economic values, investments, and productivity. Restlessness and irresponsible attitudes can negatively affect these values. Ethical maxims like prudence, benevolence, and equity are self-explanatory, applicable to human conduct, while aesthetic judgments, good faith, humanity, and social affection are also considered to be important for companies and banks.

Private banks, industrial, commercial, and holding companies frequently engage in unethical conduct, particularly in credit, savings, and securities business, often influenced by

securities firms' new products and services.

Micro services break applications into independent services, offering flexibility, faster development, and resilience. Common protocols include REST and gRPC, essential for complex systems like e-commerce platforms.

The rise of IoT devices has boosted the need for edge computing, where data is processed for time-sensitive applications. Reducing data transfer across networks, enabling efficient processing and storage of real-time data generated by IoT devices.

Modern information systems use robust cybersecurity measures, including Zero Trust Architecture, to protect sensitive data and maintain system integrity, requiring rigorous verification for access. Poor accounting methods, missing information, false declarations, goods in transit, and collaboration with auditors lead to significant errors in the banking business, resulting in fraud opportunities. Accountability is crucial for democratic order, requiring fair, non-favoritism processes and in the financial wrongdoings; which can be achieved by promoting business ethics and moral conduct. Businessmen often extract heavy loans from banks, often using hidden companies for bungling acts.

REFERENCES

- [1]. A. A. Malik, W. Azeem and M. Asad, "Online shopping, Cyber frauds and Fraud Prevention Strategies", *International Journal for Electronic Crime Investigation*, vol. 8, no. pp. 49-56, 2024.

- [2]. A. A. Malik, M. Asad and W. Azeem, "To Combat White Collar Crimes in Public and Private Sector and Need for Strong Legislation and Ethics", *International Journal for Electronic Crimes Investigation*, vol. 4, no. 3, pp. 1-8, 2020.
- [3]. A. A. Malik, M. Asad, W. Azeem, "Bank Frauds Using Digital Devices and the Role of Business Ethics", *International Journal for Electronic Crimes Investigation* vol. 2, no. 4, 2018.
- [4]. Y. Maleh, "I. T. Governance and Information Security", *Tylor and Francis*, vol.6, no.5, pp. 34-42, 2022.
- [5]. R. Anderson and T. Moore, "The Economics of Information Security." *Science and Engineering Ethics*, vol. 12, no. 4, pp. 609-632, 2006.
- [6]. R.A. Battalion, "The Financing of Terrorism: A Global Perspective." *International Journal of Law and Management*, vol. 54, no. 4, pp. 246-258. 2012.
- [7]. W. Enders and T. Sandler, "The Effect of Terrorism on the Domestic Economy: The Case of the United States," *Journal of Economic Perspectives*, vol. 10, no. 3, pp. 143-166, 1999.
- [8]. N. Kshetri, "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives," *Journal of Business Research*, vol. 63, no. 12, pp. 1255-1261, 2010.
- [9]. P. Vanini, S. Rossi, E. Zvizdic and T. Domenig, "Online payment fraud: from anomaly detection to risk management", *Financial Innovation*, vol. 9, no. 1, pp. 66-71, 2010.
- [10]. A. Ali, S. A. Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser and A. Saif, "Financial fraud detection based on machine learning: a systematic literature review", *Applied Sciences*, vol. 12, no. 19, pp. 37-48, 2022.
- [11]. I. Meghana, B. P. Venkatesh, G. K. Ganesh, N. Sumant, and R. T. Teja, "Prediction of Financial Crime Using Machine Learning", *International Journal of Innovative Research in Computer Science & Technology*, vol. 11, no. 3, pp. 96-100, 2023.
- [12]. V. Nasteski, "An overview of the supervised machine learning methods", *Horizons*, vol. 4, pp. 51-62, 2017.
- [13]. M. Hassan, C. Veena, A. Singla, A. Joshi, and M. Lourens. "Fraud Detection in IoT-Based Financial Transactions Using Anomaly Detection Techniques", *International Conference on Advances in Computing, Communication and Applied Informatics*, pp. 1-6, 2024.
- [14]. A. T. Kiyani, A. Lasebae, K. Ali, and M. Ur-Rehman, "Secure online banking with biometrics". *International Conference on Advances in the Emerging Computing Technologies*, pp. 1-6, 2020.
- [15]. Y. Abakarim, M. Lahby, and A. Attioui, "An efficient real time model for credit card fraud detection based on deep learning", *International conference on intelligent systems: theories and applications*, pp. 1-7, 2018.
- [16]. L. Baker, "The impact of the General Data Protection Regulation on the banking sector: Data subjects' rights, conflicts of laws and Brexit", *Journal of Data Protection*

and Privacy, vol. 1, no. 2, pp. 137-145, 2017.

[17]. H. Tanaka, K. Matsuura and O. Sudoh, "Vulnerability and information security investment: An empirical analysis of e-local government in Japan", *Journal of Accounting and Public Policy*, vol. 24, no. 1, pp. 37-59, 2005.

[18]. E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Electronics*, vol. 11, no. 20, pp. 33-40, 2022.

[19]. V. Zhu, "Research on Intelligent Financial Statement Analysis and Anomaly Identification Techniques by Fusing Multi-source Data". *Journal of Electrical Systems*, vol. 20, no. 10, pp. 927-941, 2024.

[20]. A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques", *IEEE Access*, vol. 11, pp. 188-203, 2023.

[21]. A. M. Mubarek and E. Adalı, "Multilayer perceptron neural network

technique for fraud detection," *International Conference on Computer Science and Engineering*, pp. 383-387, 2017.

[22]. M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika and E. Aswini. "Credit card fraud detection using random forest algorithm", *International Conference on Computing and Communications Technologies*, pp. 149-153, 2019.

[23]. P. Sood and P. Bhushan, "A structured review and theme analysis of financial frauds in the banking industry". *Asian Journal of Business Ethics*, vol. 9, pp. 305-321, 2020.

[24]. F. M. J. Teichmann and M. C. Falker, "Cryptocurrencies and financial crime: solutions from Liechtenstein", *Journal of Money Laundering Control*, vol. 24, no. 4, pp. 775-788. 2021.

[25]. N. Carneiro, G. Figueira and M. Costa, "A data mining based system for credit-card fraud detection in e-tail", *Decision Support Systems*, vol. 95, pp. 91-101, 2017.



**International Journal for
Electronic Crime Investigation**

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

DOI: <https://doi.org/10.54692/ijeci.2024.0803208>

Research Article

Vol. 8 issue 3 Jul-Sep 2024

Live Memory Forensic: Capture and Analyzing Volatile Data

Rabia Mehmood and Zohaib Ahmad

Department of Computer Sciences, COMSATS University, Lahore

Corresponding author: rabiamehmoodciit@gmail.com

Received: Aug 08, 2024; **Accepted:** Aug 28, 2024; **Published:** Sep 12, 2024

ABSTRACT

As almost 90% of malware is resident in memory, live memory forensics is an essential part of cybersecurity. Live memory forensics refers to the process of analyzing computer RAM or volatile memory (which is lost after rebooting) while the computer is running. This article provides depth on live memory forensics, which is key in the detection and analysis of cyber threats and forensics investigations. Case studies and actual events demonstrate how this method can detect unauthorized access and discover hidden malware, which will help law enforcement investigators. The practical uses of Live Memory Forensics are illustrated using real world examples. Currently, live memory forensics are faced with the temporal nature of volatile data, other technical challenges, the instantiation of indirect data related to data privacy, and evidence handling problems. The paper emphasizes the importance of moral attitude and careful handling of data to keep the forensic process incorrupt. Investigators and cybersecurity professionals should now have a good understanding of live memory forensics and how to utilize live memory forensics to enhance security across borders, not just as a detective technique.

Key words: malware, Volatility, FTK Imager, Live Memory Forensics, incorrupt, data privacy, evidence handling.

1. INTRODUCTION

However, live memory forensics is the approach used to capture and inspect the temporary data stored in a computer's RAM (Random Access Memory) when the system is up and running [1]. This type of forensics allows the researcher to capture a snapshot of the current state of the system, with all processes active, modules loaded, user interactions and network connections. Memory Captured RAM is used for storing pieces of information the computer needs while running, like open files and running software [2]. Unlike data stored on nonvolatile storage such as hard drives, the data in RAM is lost when the system is powered off, which is why it is memory capture is crucial for preservation of temporary data. Volatile data refers to data that is stored temporarily in a computer system's Random Access Memory (RAM). Memory/memory utilization/CPU/memory/CPUS tats/active applications, threads and system processes, Sessions and connection of a network, Operating System Functionality and Transient Storage. Volatile data is transitory, meaning it is available only while the system is in operation [3]. Typically, this data is lost when the system is shut down or rebooted, which is why we need to capture the live data during search/investigation. Importance of Volatile Data in Digital Investigations: In numerical surveys, volatile data is important for a few reasons: Transactional Awareness: Transitional data provides an instantaneous snapshot of the operations running on a system, allowing researchers to identify what was running on the machine at the exact

moment of capture. This includes monitoring user activity, network communication and the process runtime. Which would tip them off to unauthorized access. Advanced threat detection: Advanced threats such as rootkits and malware often reside in memory and evade discovery by traditional file-based antivirus scans [4]. Researchers can investigate these in memory threats which do not appear on hard drives by analyzing volatile data [11]. Malevolent actors also hide their activities, either through in memory execution or code injection. Such unseen actions can be captured using Live memory forensics, which examines the contents of RAM, including hidden processes and injected code. Sensitive Data Retrieval: Sensitive data, including encryption keys, decrypted content, and passwords, often resides in memory [5]. Retrieval of this data can be critical for determining the magnitude of security incidents, recovering ransomware data, and identifying compromised credentials. This means that while using the exec option allows copying the memory through every exec call because it saves the processor state and system setup (acpile polled, for instance), volatile data covers other data related to the exact state of the system: system configurations, memory mappings, kernel internal structures. This data helps forensic experts to comprehend the network implementations where an assault took place and to evaluate the overall damage to the system(ii) Capture app install | the full hardware property data. It is required to track the current information only through the given tools, we can get the data. Signs because live memory forensics is

important: Live memory forensics is important for locating indicators that are not even stored on a hard disk. Hoo Tem Forest Encapsules about Traditional Forensic is defined by a scope that goes back to the age of when. Low levels, in particular, include the existence of data in the file system and various file systems and the detection of random data. However, many crucial pieces of evidence exist only in RAM, which dissipates when the computer is powered off. Researchers are, therefore, able to analyze or take snapshots of live memory to: Detection of active rootkits & malware: Identify data exfiltration attempts and immediate network connectivity, Check system interactions & user interaction, this form of live memory forensics is a live investigational procedure in the modern digital obehilton. It brings insights that contrast traditional forensic analysis, enriching a theoretical approach to cyber incidents.

2. METHOD AND MATERIAL

2.1. Live Memory Forensics Basics

Live memory forensics is a sub analysis for digital forensics in which the volatile data resident in a computing system is analyzed and extracted while the system is still running. This provides researchers with a snapshot of the system's current state in real time and captures important information that may not persist on the disk.

2.2. Volatile Data

The data that is stored temporarily in the RAM (Random Access Memory) of a computer is referred to as volatile data. It holds information on loaded modules, network connections, system processes, user activities, active processes and the temporary files used

by the Operating System. The volatile one is data available in memory only, and it is lost when the system loses power or restarts. It is a solution that means the data is stored on nonvolatile storage devices like hard drives or SSDs.

2.3. Importance of Digital Investigations

Live memory forensics is necessary in digital investigations because it can acquire live artefacts that are critical for the detection of malicious activities and for understanding system interactions. Through the examination of volatile data, forensic experts can identify open network connections, memory resident malware, and live processes that old antivirus programs could miss. This forensically sound scanning triggers the preservation and extraction of vital evidence, which constructs a timeline and restores digital events and prevailing lawful records.

2.4. Tools and Techniques

Researchers make use of specific tools and techniques to carry out live memory forensics in the most optimum way. Volatility Framework isolates forensic traces in volatile memory [6], memory imaging and memory dump analysis for controlling tools. It also supports many operating systems (architectures) That give forensic experts great power to analyze memory fillings and find hidden processes. Remembering, the different noticeable instruments offer progressed memory examination functions that are more suited for free examination than custom personalized memory procurement for complex forensic circumstances. Redline, founded by FireEye [7], provides automated memory forensic analysis and detection of malicious software and activity, allowing

cybersecurity incident response and operations teams to perform rapid response.

2.5. Live Memory Forensics

Methodologies

The technique of performing live memory forensics [8] is made up of multiple important steps. Forensics analysts first record a memory dump or image with tools like Volatility Framework or FTK Imager. The method is responsible only for capturing the live memory data, which is stored in the Eccentric RAM, including the system artefacts, network connections, processes, etc. The researcher then performs detailed memory dump forensics by identifying the IoCs mentioned above and producing a timeline using signature based scanning and string searching [10]. This method allows analysts to recreate online interactions, identify security violations, or collect proofs needed for cybercrime investigations.

2.6. Applications in Cybersecurity

Live memory forensics is a very powerful tool for incident response and Threat detection in Cybersecurity. By analyzing and collecting volatile data live, cyber security professionals can rapidly identify and remediate incidents such as APTs (Advanced Persistent Threats), security incidents, data breaches, and insider threats. This pragmatic measure strengthens the ability of the organization to recover from cyber threats quickly and reduce the impact of security breaches on critical systems and data. Moreover, live memory forensics enables practical threat hunting activities by assisting analysts in uncovering and mitigating early-stage threats before they escalate into silver platter attacks.

2.7. Challenges and Considerations

As with any great reward, live memory forensics is not without its own set of challenges and considerations. If data is located in RAM, volatile data can be quickly lost if it is not detected in time. Furthermore, ethical and legal considerations also make it necessary for forensic professionals to convey sensitive standards of privacy and indication heading. Moreover, the sophistication of these memory structures and the sheer amount of data the investigations produced created unique challenges and required scientific abilities and understanding.

3. SIGNIFICANCE

Live memory forensics is an important focus of Cybersecurity and digital forensics. It provides a snapshot of data in a computer's RAM without needing to cease the system. The technique is important for cyber security people and digital forensic researchers to improve digital investigation, malware analysis, and incident response.

3.1. Incident Response

Live memory forensics is valuable in incident response scenarios with the need for quick action. Real time analysis and capture of volatile information are needed to help cybersecurity teams identify network connections, memory resident threats, and active processes during a security breach or suspected malware attack. Such a practical methodology enables organizations to surround the event on the go without letting it escalate and without risking any sensitive data.

By analyzing the volatile data in the RAM, detectives can piece together a sequence of events before and during the incident. This skill is invaluable when considering event likelihood, understanding attackers' entry methods,

or communicating effective response measures. Developing an analytical model that can quickly identify the event allows a company to isolate it before it disrupts the normal business process, resulting in the smallest possible economic and reputational loss.

Live memory forensics is a very integral part when it comes to the analysis of malware as it works especially well in the case of hunting memory resident complex threats. Traditional malware detection methods, like signature-based antivirus solutions or static file analysis, can easily miss memory resident malware that silently remains hidden while it performs its actions.

Forensic analysts learn live memory forensics tools to capture and analyze volatile memory. This lets them spot bad processes in action, help them abstract out IoCs, and track the malicious process as it performs its actions. By reverse engineering malware memory interaction, experts uncover the malware's persistence mechanism, command and control communication channels, and impact on the compromised environment.

3.2. Unauthorized Access Detection

They use live memory forensics to detect unofficial access attempts and internal threats. Monitoring memory actions in real time allows administrators to detect out of the ordinary user behaviour, unauthorized network connections, or unusual processes a signal of a security compromise. This security monitoring helps improve the cybersecurity posture by quickly identifying and responding to potential threats, which reduces the chance of data loss and insider attacks.

If an attacker demands temporary access which they do most of the time they need to run a process or two to execute a network connection, followed and usually partially littered with strange process executions or state sponsored memory feasting processes that linger in volatile memory and leave traces. Live memory forensics allows forensic experts to detect those traces and identify them to assess the potential and impact of unauthorized access events. Prompt ID and response to those events are needed to stop the bleeding, comply with regulatory requirements, and correlate to sensitive info and data exfiltration.

3.3. Applications of Live Memory Forensics

Live memory forensics serves as an important tool for collecting illegal evidence and reconstructing digital crime scenes in digital investigations. The volatility data surveillance with memory dumps allows forensic experts to establish timelines, reenact user action and search for malevolent elements. Crucial to legal records, this forensic evidence provides the physical evidence that will prove unauthorized entry, data exfiltration, or other cybercrimes leading to a long day in court as law enforcement carries out its exhausting role and ensures that accountability is procured.

Digital investigations frequently involve forensic analysts examining the system at a particular moment in time to piece together the sequence of events by which a threat actor carried out their actions. Live memory forensics allows us to capture a memory image of the system in a live state. It can be used in cases where a system is going to be shut down or rebooted, where evidence can

degrade in system memory. It integrates multiple related artefacts to support comprehensive investigations and comprehensive documentation of digital incidents to help make informed decisions and prosecution efforts.

3.4. Boosting Cybersecurity Level

Live memory forensics helps boost the cybersecurity level, providing visibility into real time data breaches and detecting threats proactively. By capturing and analyzing volatile data, organizations can take immediate action in incident response, including identifying the threat, preventing its spread, and preventing future attacks. By incorporating live memory forensics into cybersecurity procedures, incident response efforts become more robust, threat detection more precise, and key systems and data more resistant to the diverse swath of security threats that are now commonplace.

Leveraging live memory forensics proactively allows organizations to uncover and mitigate new threats instantly, shortening attacker dwell time on their networks and lessening the implications of security incidents. Some actionable insights that can be derived with the help of volatile data in real time include the ability to detect indicators of compromise (IOCs), catch stealthy malware infections that might go undetected otherwise, and help prevent exposure to attacks by unauthorized means before they eventually snowball into full blown breaches.

3.5. Understanding Tools and Techniques of Memory Capture

Memory images themselves are foundational to live memory forensics, the practice of reading volatile data from a computer's RAM during active operation. This section will present

major tools for memory image capture and explore the roles they have in a digital investigation.

The FTK Imager is a tool that assists in capturing and analyzing disk and memory images created by the Access Data Team. It has an intuitive interface and works with a wide range of file types (DD (raw), E01 (forensic image), and AFF (Advanced Forensic Format)). With FTK Imager, forensic analysts can perform live memory forensics to /capture volatile memory snapshots with acquired active processes, network connections, and loaded modules.

To capture memory with FTK Imager, the examiner usually boots the application on the target system or remotely, chooses "Capture Memory," and then specifies the location and the desired output format. The solution pronounces a memory dump file containing important information, which can be analyzed to affirm evidence of manipulative activities or a system compromise.

Belkasoft Live RAM Capturer is a tiny, free, standalone executable that enables you to focus on obtaining live memory images in a condition as close to the original as possible, without even USB drives because the memory conservation feature is provided in the most similar way to a hibernation file on both 32 and 64 bit systems. Belkasoft Live RAM Capturer is widely known for its ability to guarantee flawless functionality and minimal system load, ensuring rapid and reliable acquisition of volatile data. Belkasoft Live RAM Capturer allows forensic specialists to create memory dumps of the working processes of the computer, as well as to obtain data on operating network connections and operating system registry records. Its

advanced memory acquisition techniques for data integrity allow full forensic analysis and evidence recovery by those trained in its use.

An open source Memory Dumper by Moon Sols is very popular among digital forensics investigators for capturing the memory of Windows operating systems. Its simplicity and reliability make it great for capturing memory snapshots in a live forensics scenario without disrupting the volatile memory state.

In general, a forensic analyst or IT security researcher will run the tool against a system of interest, providing a path for the output memory dump file, and letting it grab the contents of physical memory. The resulting file dump has some vital artefacts that can be analyzed using forensic tools to check for malware infection, unauthorized access attempts, or any other suspicious activities.

3.6. Choosing the Right Tools for the Right Jobs

While choosing a memory capture tool for live memory forensics, analysts look at many factors, such as target OS compatibility, Capture method, i.e., physical vs. virtual memory, preferences for output format, and, most importantly, integration capabilities with forensic analysis platforms. Every tool has its strengths and points to consider depending on the investigation requirements or type/characteristics of the target system.

Tools such as FTK Imager [9], Belkasoft Live RAM Capturer [12], and DumpIt are famous in the world of live memory forensics. They produce excellent results in acquiring and preserving volatile data for analysis. Their use allows forensic practitioners

to collect the valuable evidence they need to build a case for legal action, respond to an incident, or take cybersecurity precautions.

4. STEP BY STEP CAPTURING OF VOLATILE DATA

Live memory forensics allows investigators to gather real time data stored in a computer's RAM while the computer is running. This step-by-step walkthrough illustrates how to use Volexity Capture to capture volatile data for forensic analysis safely and effectively.

4.1. Preparation and Planning

Target System Identification: Choose the target system from which you wish to acquire volatile data. If your remote access is needed, deploying Idea Scale V2 must be configured as a system and ready to go on the network.

Choose The Capture Tool: Select a memory capture tool like FTK Imager, Belkasoft Live RAM Capturer, or DumpIt [13] that is compatible with the target system and the investigation requirements.

Prepare Storage and Environment: Reserve adequate storage for the memory dump file to avoid interference during the capture process and ensure a safe and distraction free capturing environment.

4.2. Run Memory Capture

Start the Capture Tool: The capture method you selected will determine how you start the memory capture tool, either on the target or remotely (if the tool supports that and you have the necessary permissions).

Capture Settings Configuration: Use the below settings in the tool to configure the capture settings, such as where to select the memory (either

physical or virtual) to capture and what should be the output format and path for the memory dump file.

4.3. Start memory capture in the tool

Run the tool and take a snapshot of the volatile data stored in the system's RAM. The time the capture will take depends on the tool's memory size and efficacy.

4.4. Verify and Validate

Validate Data Integrity: Ensure that the collected memory dump file contains complete and correct volatile data of the target system.

4.5. Validate Against Source

The captured data should be compared to the live system to verify that the snapshot of memory correctly represents the system's state at that time.

Capture Details: Write down important information like the time of capture, the duration of capture, the tool used in the capture and any other information about the capture observations, system condition, etc.

4.6. Analyze and Interpret:

Forensic Analysis Tools: Move the memory dump file to a forensic analysis workstation with tools like the Volatility Framework, Magnet AXIOM, Encase Forensic, etc. These tools help in depth analysis and extraction of artefacts from the captured memory.

Retrieve Significant Artifacts:

Extract and investigate artefacts from the memory dump file, such as active processes, network connections, loaded modules, set registry keys, and user actions. Spot any oddities or Indicators of Compromise (IOCs) that may suggest security attacks or evil activities.

Document Findings: Enter your findings in a structured way, including artefacts, time stamps and how they relate to the investigation. Keep clear and comprehensive logs to support forensic analysis and potential criminal proceedings.

4.7. Secure and Preserve

Protective Storage: Save the memory dump file and generated analysis in safe and controlled storage to avoid unauthorized tampering with the generated data.

Chain of Custody: Follow the chain of custody principles to ensure that evidence is preserved in a way suitable for use in court. Capture all handling and transfer activities of the memory capture and associated data.

5. EXAMINE CAPTURED IMAGE AND MEMORY

This is the most important phase in live memory forensics, and it allows forensic investigators to extract and interpret volatile data from dumped memory images taken from a live running system. This part details the process of memory dump analysis through Volatility and Rekall, providing the reader with the ability to perform some basic memory dump examinations, such as listing running processes, network connections, and other types of malicious indicators.

5.1. Using Volatility

Volatility is a popular open source memory forensics framework that uses memory dumps to analyze memory in memory related forensic investigations. It comes with a ton of plugins specifically designed to pull out different forms of information from memory images, such as running processes, network connections, loaded modules, and registry keys.

Step by Step Process:

Environment: Move the image file to a forensic analysis workstation with Volatility installed. Safe and seclusion of the environment to avoid contaminating or tampering with evidence.

Choose the Best Plugins: Identify and choose the right Volatility plugins for some of the artefacts you need to analyze. Common plugins are pslist (list processes), netscan (list network connections), malfind (find injected code), and ldrmodules (list loaded modules).

Run Volatility Commands: Execute Volatility commands with chosen plugins on the memory dump file.

Analyzing Output: Reviewing the output of the Volatility commands to extract relevant artefacts and data. It determines running processes, checks for unknown or suspicious programs, monitors network connections and evaluates loaded modules for potential signs of malware.

Correlate Data & Interpret Data: Correlate findings across different volatility plugins to build a unified picture of the system's state at the time of memory capture. Examine identified artefacts with the investigation goals in mind to determine potential security incidents or indicators of compromise (IOCs).

5.2. Using Rekall

Rekall (Now Plaso) is a second dominant framework (rekall) that supports the analysis of memory images across different platforms. It provides a scalable/extensible platform for analyzing memory dumps and taking out useful information from it.

5.2.1. Step by Step Process

6. RESULTS AND DISCUSSIONS

Real Life Case Studies

First, you need to set the Rekall Environments, which means Installing and configuring Rekall on the memory dump file analysis workstation. Then, you need to match the format of memory dumps with its architecture.

Profile: Create a Rekall profile for the particular operating system and version from which the memory dump was taken. E.g., profiles) is that which tells Rekall about how it should interpret memory structures and data formats.

Investigate the memory dump: Load the memory dump file using the correct profile in Rekall. Rekall Commands and scripts used: Rekall Lin Profile memory filename D drivers profile mainline pgx32 hives can list |> /root/VikingTools.py

Perform Analysis Tasks: Issue Rekall commands to examine which processes are running (pslist), network connections (netscan), loaded modules (ldrmodules) and registry keys (hivelist).

Rekall Command Output Analysis and Interpretation: Analyze Rekall Command output to ascertain relevant artefacts along with potential security issues. Compare the ground cinnamon to other forensic discoveries to construct a timeline and reenact the events leading up to the incident.

Using these tools, memory images can be analyzed comprehensively, extracting important forensic artefacts and revealing the activities of an attacker or breached organizations. This is the ideal class of tools for aiding investigative efforts and bolstering Cybersecurity and the legitimacy of digital forensic examinations.

Finally, practical examples in real cases will show us how useful live memory forensics are and their effectiveness in

dealing with ongoing cybersecurity incidents. The following section illustrates some of the important scenarios where live memory forensics was essential in identifying, investigating and responding to different types of cyber threats.

Case Study 1: Cyber Attack on Financial Institution

One of the largest financial institutions was facing a sudden surge of suspected network activities, signalling a potential data breach. Forensic analysts used a live memory forensics tool like Volatility to extract memory dumps of the compromised systems. Examination of the evidence discovered further that the attackers had used stolen credentials for initial access. Also, that code designed to evade traditional, signature based security controls was being employed. The institution used memory analysis to identify the attack and address it with confidence for spotting and to respond to the threat, thwarting further exfiltration and hardening itself against similar future attacks.

Case Study 2: Healthcare Malware Incident:

The client was a healthcare facility that recently had an issue in which its malware antivirus protection system failed. Another healthcare organization was rattled by a significant malware outbreak, which disrupted critical systems. We used live memory forensics tools, such as Rekall, to take memory dumps from affected endpoints. Investigations showed that legitimate applications were being injected by malicious processes that were trying to get access to patient records and healthcare information. Examination of volatile data

determined the malware's persistence and C2 communications, allowing the organization to contain the infection, prevent or limit the loss of PII/PHI, and implement improved security to protect patient privacy and operational capacity.

Case Study 3: Insider Threat Detection at a Technology Firm

Suspected unauthorized data access and leakage by an insider in a technology firm background to a corporate espionage investigation. Live memory forensics was pivotal to retrieving volatile content from the suspect's workstation while it was being used. Memory dump analysis, on the other hand, disclosed access to requested confidential project files and suspicious network activity characteristic of data exfiltration cascades. A thorough analysis of the volatile data ended up giving valuable evidence that positioned the actions of the insider as the cause of the security breach, which enabled prompt decisions on disciplinary consequences and improved internal security guidelines to prevent new threats from within.

Example in the Real World of Government Agency Cyber Attack

Hackers launched a well-crafted cyber-attack against a government agency to compromise classified national security information. Live memory forensics allowed us to dump the memory of the compromised system and find IOCs associated with APTs. Advanced forensic analysis revealed the presence of stealthy malware implants, zero-day exploits, covert malicious communications, and other advanced malware loads used for illegal activities. Identifying and responding to

the volatile data allowed the agency to close vulnerability gaps used by the adversary, minimizing the extent of the breach, limiting the impact and hardening its cyber security posture from penetrations posed by persistent and emerging cyber threat actors holding government and critical infrastructure adversaries in their target list.

Retail Sector Data Breach (Real World Example)

Data Breach for A Leading Retail Corporation, Exposing Sensitive Payment and Corporate Data Live memory forensics tools were used to capture memory dumps from infected point of sale (POS) systems and device servers. The forensic examination of volatile data identified malware specifically designed to collect and then transmit payment card data from transactions where its rupture point was intercepted from the POS software. Investigators used forensic analysis of memory artefacts to identify the malware's activities, found the systems affected, and took immediate action to halt unauthorized data access, alert the affected customers, and meet regulatory reporting requirements.

The value that memory forensics brings to modern cybersecurity operations becomes very clear when we review these case studies and real world examples. Forensic analysts detect, investigate, and mitigate cyber threats by capturing and analyzing volatile data from systems that are live, all done to protect organizations from threats that can cost them money, hurt their reputations, and bring about operational disturbances. Experience With live memory, forensics often demonstrates

real importance in incident response, threat detection, and digital investigations across many industries financial, healthcare, technology, government, and retail.

Key features of live memory forensics enable organizations to proactively surveil and secure their cyber environments against the constantly evolving cyber threat landscape, resulting in resilience, robust defence capabilities, and guaranteeing the forensic soundness of investigations. Incorporating live memory forensics into broader cybersecurity operations increases the likelihood of identifying and responding to any nefarious behaviour early, preserving digital evidence and reducing the risks associated with advanced cyber adversaries.

7. CHALLENGES AND LIMITATIONS

One of the many challenges and limitations of live memory forensics, used in modern cybersecurity investigations, is making sure the forensic analyst can #1 get the information they need and #2 that this information is accurate and reliable without violating the integrity of the data present when performing a forensic investigation should it be necessary.

Data Volatility

This presents a formidable challenge for forensic investigators, and many varieties of hardware trojans persist in a computer's volatile RAM. Unlike data saved in persistent storage such as a hard drive, volatile data stored on RAM is gone when your system shuts down. Just like RAM, this means that all data in RAM is lost once the system loses power or is turned off. From the

forensic perspective, real time volatile data acquisition is very important as this provides a frozen image of the system at the time of investigation. But this also means that if the capture process is delayed or interrupted, so is the evidence, which could be crucial.

An obstacle is the fact that data remains volatile, and forensic tools and techniques are deployed in an attempt to minimize disruption during capture. Techniques, Volatility tools of Rapidly memory dump and Rekall.execSQL. It is a very fast way to create memory dumps with both tools. These dumps take an image of the currently running processes, all network connections and other volatile data on the RAM. Swift and accurate capture of the data allows forensic analysts to maintain the integrity of the evidence and recreate the events on the victim system.

Potential Contamination

Another important problem is the corruption of volatile data during forensic analysis. Forensic analysts should be careful not to modify or taint memory contents. Analysis of live memory may be subject to inaccuracies due to some factors, i.e. malware in memory. These on disk memory analysis tools change data in memory or artefacts incorrect detection because some processes can be active and modify data. To minimize this risk, we outline some of the strict protocols we adhere to, such as the use of credible forensic tools, verification and validation of forensic tools, verification of memory image integrity via checksums, and finally, chain of custody documentation.

Furthermore, forensic analysts implement methods to ensure the

system is not significantly affected during data acquisition. Therefore, anything operating within volatile memory, such as memory only live forensics, can never contaminate disk storage, and the integrity of volatile data can be obtained directly without time consuming and unreliable methods of extraction. These are intended to protect the collected evidence from being invalidated in case of legal issues, which thus further enables the evidence to still come out as actionable intelligence usable for cybersecurity incident response.

Legal Considerations

Privacy Rights Data Protection Regulations Admissibility of Evidence in court and more. The process of collecting and analyzing volatile data is a sensitive topic as it has to do with volatile memory, which may contain personal data, user communications, and sensitive business data. Those performing live memory forensics need to abide by constraints imposed by law concerning data privacy and electronic evidence.

Legal issues

Making sure data is legal to be collected, have a chain of custody and privacy agendas are defined. For example, jurisdictions could implement regulations around how long data could be retained, how data needed to be secured, and how consent was to be achieved before accessing and analyzing volatile data. Noncompliance with these legal mandates may then potentially preclude forensic evidence from entering, effectively nullifying the utility of live memory forensics as an investigative tool.

7.1. Technological Limitations

Cybersecurity investigations are also impacted by technological limitations that make live memory forensics much less effective. Different computational environments use different hardware architectures, operating systems, and memory management, and these differences make it difficult for forensic tools and methods to produce constant output. The forensic analyst should have a sufficient understanding of the underlying behaviours of these complexities and should evolve their methodology to be sustained to maintain forensic soundness and reliability.

In addition, cyber adversaries are highly developed, which adds complexity to live memory forensics. Prolific malware techniques such as file less malware and antiforensic methodologies can also avoid detection and control from forensic tools. Polymorphic ransomware is particularly problematic because of the ease with which it can be customized to elude existing security measures, and spotting them is virtually impossible without forensic capabilities, ongoing research and information sharing among organizations in the security community to create the necessary countermeasures and detection techniques.

Mitigation Approaches for the Real World:

To effectively address these challenges and limitations, organizations and forensic analysts can follow some pragmatic strategies:

Training and Certification: Regular training and certification in live memory forensics keep forensic

analysts current with the tools, techniques, and legal prerequisites.

Validation and Utilization of Tools:

Use verified and trusted forensic tools, ensure the tool is competent with every other operating system, and test the tool to validate its efficiency.

Evidence Records: keeping detailed records of how evidence was accessed, ensuring the integrity of the evidence so that it can be presented in court

Legal Proficiency: Working with legal experts of the company to cope with the regulatory environments, solve problems by keeping privacy intact and also complying with the data protection laws.

Stakeholder Standpoint: Continue monitoring technological development, researching new threats, and adapting forensic techniques so that detection and analysis capabilities remain up to date.

The practices mentioned here (among many others) will help organizations carry out better live memory forensics, thereby reducing accompanying risks and elevating the cybersecurity posture against emerging Cyber threats.

ETHICAL AND LEGAL ISSUES

The technique of live memory forensics in the investigation of Cybersecurity is important but also full of legal and moral pitfalls that must be complied with to preserve a correct forensic process and respect the rights of the individual. This section examines the ethics and legal issues of capturing and analyzing live memory data and the need for compliance in this area.

7.2. Ethical Implications

In the world of live memory forensics, ethicality is the primary concern with privacy, data confidentiality, and the

sensitive information being processed being handled responsibly. While pulling up live memory captures, forensic analysts can see a broad swath of volatile data, including personal communications, websites visited and patterns of application usage. To keep forensic investigations ethically sound and professionally set, respecting the privacy of individuals and maintaining confidentiality are the most important factors.

Forensic analysts must have proper analysis consent to access volatile data, especially in corporate and legal settings. Transparent data collection practices also help build trust and accountability by making people more fully aware of when and for how long all forensic investigations are taking place. Forensic examiners should also adhere to the concept of data depreciation, which is to say that they should only gather and preserve the necessary volatile data to avoid privacy implications and to conform to ethical guidelines.

One strong point is associated with the ethical consideration of negative externalities that come to the subject of forensic investigations in the form of people or organizations. The application of live memory forensics, in this case, can unearth confidential information, and you never know it. Still, evidence of nuisance is also possible, which can have a stronghold upon stakeholders. Forensic analysts have to deal with the facts of cases sensitively and professionally, ensuring that they remain objective and unbiased concerning their findings throughout the process of investigation.

7.3. Legal Considerations

In live memory forensics, legal aspects refer to data protection legislation, the admissibility of evidence in court, and procedural standards and guidelines for forensic investigation. One of the numerous legal frameworks around data privacy, electronic communications, and the admissibility of digital evidence is collecting (only the most legally defensible portions) and analyzing volatile data from live systems, which is a minefield.

Forensic investigations often fall under regulations like the General Data Protection Regulation (GDPR) in the European Union or the Health Insurance Portability and Accountability Act (HIPAA) in the United States. To comply with these laws, data protection obligations, such as obtaining consent for data processing, notifying individuals when there is a personal data breach, and taking appropriate measures to ensure the security and confidentiality of personal data, are very strict.

Forensic experts may have to justify the use of a particular forensic technique in a court of law before evidence obtained using live memory forensics is admissible for the intended application.

The judiciary construes these rules as entitling volatile data to stand under the

Application of Ethical and Legal Principles into Practice

There are several best practices forensic analysts and organizations can consider when grappling with ethical and legal considerations.

Ethical Standards and Codes of Conduct: Follow professional ethical guidelines and codes of conduct, such as the IACIS or ADFSL code of ethics.

Building Trust Informed Consent and Forensic Live Memory Captures:

At the heart of any live forensic investigation is trust, Employees Individuals Stakeholders Informed Consent Asking for the consent of individuals or stakeholders aware of the potential memory capture before a forensic investigation is about to begin is critically important.

Data Protection Mechanics, which include Securing volatile data using strong encryption, anonymization, and secure storage, restricting unauthorized access, and preventing data disclosure.

We Take Legal Compliance: Seriously, We Must Stay abreast of all laws and any updates affecting forensic investigations and consult with legal experts as needed to ensure compliance.

Documentation and Chain of Custody: keeping detailed records of forensic procedures, including ensuring the chain of custody or that it has not been tampered with before legal proceedings so that the volatile data can be admitted as evidence.

If properly formalized, adopting these practices can help organizations abide by necessary ethical standards, reduce legal liabilities, and even strengthen the reputability of live memory forensics as an indispensable method in cyber security forensics.

8. FUTURE TREND

Due to the sophistication of cyber threats and the complexity of modern digital stagings, memory forensics needs to be achieved at a faster pace than traditional techniques. This paper discussed recent trends and innovative perspectives, although this portion emphasizes the improvements in memory forensics.

Recent Technological Improvements in Forensic Tools

The memory forensics tool landscape is constantly evolving, primarily based on the need to support a varied range of operating systems, architectures, and memory management methodologies. Old ones like Volatility or Rekall are still being enhanced by new functionalities that make them faster when capturing and analyzing volatile data. Advancements in these areas have included greater support for virtualized environments, upward compatibility with newer operating systems and improvements to multi core processing optimizations that make memory dump analysis faster.

Additionally, a key trend which is expected to gain ground in the memory forensics market is the growing usage of memory forensics tools by embedding machine learning and artificial intelligence (AI). Anomalous memory patterns are automatically detected and prioritized as critical findings for forensic analysts by using AI algorithms. It takes the burden off analysts, makes the entire investigative process more efficient and augments the capability to uncover advanced, stealthily in memory malware.

EDR Integration

Memory forensics is merging with Endpoint Detection and Response (EDR) solutions. Transforming how Organizations are defending themselves against cyber threats. Now, EDR platforms support memory file forensics so that during a security breach or incident, memory snapshots can be collected and stored for later analysis. The integration helps to perform real time threat hunting, fast

incident response, and link memory based artefacts to endpoint behavioural data.

Utilizing EDR integrated Memory Forensics can increase organizations' insight into memory resident threats (e.g., Fileless malware, and APTs). This keeps dwell time to a minimum and damage low while improving security resilience against new threats.

Virtualization and Cloud Forensics

The emergence of cloud computing and virtualization creates new difficulties and opportunities for memory forensics. Cloud based memory forensics collects and analyzes volatile data on virtual machines (VMs) and cloud instances due to the memory state of VMs running in shared environments with dynamically distributed memory resources. Forensic analysts are developing special tools and techniques to address the unique challenges of cloud memory forensic areas such as data isolation, chain of custody preservation across virtualized environments, and legal issues relevant to cross border data transfers.

Cloud native memory forensics tools are likewise advancing, allowing organizations to naturally extend their investigatory prowess into the cloud and cloud based workloads and applications. These tools cover functionalities like capturing memory dumps from cloud instances and remote memory analysis, and they integrate with cloud security platforms for coordinating response actions across expanded environments.

Privacy Preserving Techniques

Introduction Privacy concerns and regulatory requirements are forcing memory forensic practitioners to learn

privacy preserving techniques. Increasingly, forensic tools are embedding encryption and anonymization technology to safeguard sensitive data that can be protected at the time of data capture, storage, and analysis. By doing so, you can prevent unauthorized access or leaks of personal and sensitive data and avoid fines under data protection laws like GDPR and HIPAA.

In addition, innovations in differential privacy and secure Multiparty computation seek diverse ways to reconcile forensic access with privacy rights. This provides forensic analysts with the channels to fully investigate without risking the identity and security of persons connected to legal and corporate inquiries.

Future Dangers and Safeguards

As we move forward, memory forensics needs to keep up the pace of new methods and tools adversaries can and will use to evade and hide their malicious activity. At the same time, threat actors are using increasingly sophisticated obfuscation tools, anti-forensic techniques and memory resident malware aimed at escaping the detection and manipulation of traditional forensics approaches. Overcoming these limitations will be the main areas of research for future memory forensics development as we move towards both proactively detecting threats, refining memory introspection procedures, and incorporating real time anomaly detection algorithms.

Through this solution, forensic analysts can proactively detect and respond to threats in real time using behavioural analysis and machine learning driven

techniques, eliminating security gaps and reducing organizational risk. Collaborative research and information sharing among the cybersecurity community best position memory forensics capabilities to address the propagations associated with today's fast changing threat landscape.

9. CONCLUSIONS

Live memory forensics is really important in Cybersecurity because it allows you to recover volatile data from the RAM of a computer, which could be evidence that is not stored on hard drives and other storage that typically only is used to store data but not to process it. This process is important in the field of digital forensics as it gives an instantaneous picture of the state of a system, which includes active processes, network connections, and users. Appreciating the basics of live memory forensics is essential as it provides forensic analysts with the essential knowledge and resources to carry out comprehensive investigations efficiently. FTK Imager, Belkasoft Live RAM Capturer and DumpIt are some of the essential tools available for efficiently capturing memory images that secure the evidence for legal and corporate investigations. Live memory forensics is an essential tool used in Cybersecurity in areas such as incident response, malware analysis, unauthorized access detection, and search for insider threats. Emphasizing the incidents in which live memory forensics is crucial, organizations can improve the depth and efficiency of their cybersecurity defences and their capacity for rapid and effective response to security incidents. This practical knowledge of tools and their

methodologies enables forensic analysts to manoeuvre complex digital environments with accuracy in compliance with forensic best practices and legal standards. A step-by-step way of taking volatile data from any forensic related activity, which provides a definite systematic process for why and how to execute memory dump on any running systems. This procedural guidance is key in making certain that forensic practitioners follow the proper data handling practices to keep the evidence maintained to its integrity and admissibility in a legal setting.

REFERENCES

- [1] I. Taha, M. Mirhassani, and A. E. Analog, "A Monotonically Linear DCO for 77 GHz Automotive Radars," *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, Windsor, ON, Canada, pp. 77–80, 2018.
- [2] M. M. Rahman, M. M. Hossain, and K. K. Karmakar, "I shape microstrip antenna design for WiMAX, Wi Fi and biomedical application at 2.45 GHz," *2013 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, India, pp. 546–549, 2013.
- [3] S. I. Md Salim, H. A. Sulaiman, R. Jamaluddin, L. Salahuddin, M. N. S. Zainudin, and A. J. Salim, "Two pass assembler design for a reconfigurable RISC processor," *2013 IEEE Conference on Open Systems (ICOS)*, Kuching, Malaysia, pp. 77–82, 2013.
- [4] W. Alkohlani and J. Cook, "Towards Performance Predictive Application Dependent Workload Characterization," *2012 SC Companion: High Performance*

-
- Computing, Networking Storage and Analysis*, Salt Lake City, UT, USA, pp. 426–436, 2012.
- [5] J. N. Mahajan and A. M. Jain, "Conversion of existing inverter into solar inverter," *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, pp. 859–862, 2017.
- [6] N. Kumar and S. Agarwal, "A dynamic Workload Management model for saving Electricity Costs in cloud data centers," *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Delhi, India, pp. 1246–1251, 2014.
- [7] Y. Qiao, N. Wu, C. Pan, and M. Zhou, "Petri net based response policies to process module failure in time constrained single arm cluster tools," *Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control*, Miami, FL, USA, pp. 144–149, 2014.
- [8] M. F. M. Fudzee, J. Mohamed, J. Abawajy, S. Kasim, and M. N. Ismail, "An SLA Evaluator for Multimedia Content Adaptation Services," *2014 International Conference on Information Science & Applications (ICISA)*, Seoul, Korea, pp. 1–4, 2014.
- [9] P. Ameri, U. Grabowski, J. Meyer, and A. Streit, "On the Application and Performance of MongoDB for Climate Satellite Data," *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, pp. 652–659, 2014.
- [10] V. C. Valgenti, H. Sun, and M. S. Kim, "Protecting Runtime Filters for Network Intrusion Detection Systems," *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, Victoria, BC, Canada, pp. 116–122, 2014.
- [11] Y. Tian, F. Deng, Z. Chen, P. C. Loh, and Y. Hu, "Impedance analysis of control modes in cascaded converter," *IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society*, Yokohama, Japan, pp. 003545–003550, 2015.
- [12] S. Jamalain and H. Rajaei, "Data Intensive HPC Tasks Scheduling with SDN to Enable HPC as a Service," *2015 IEEE 8th International Conference on Cloud Computing*, New York, NY, USA, pp. 596–603, 2015.
- [13] K. E. Adetunji and M. K. Joseph, "Development of a Cloud Based Monitoring System Using 4Duino: Applications in Agriculture," *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, Durban, South Africa, pp. 4849–4854, 2018.
- [14] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, pp. 124–134, 1994.
-

Editorial Policy and Guidelines for Authors

IJECI is an open access, peer reviewed quarterly Journal published by LGU. The Journal publishes original research articles and high-quality review papers covering all aspects of crime investigation.

The following note set out some general editorial principles. 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. 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 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

