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

# International Journal for Electronic Crime Investigation

# (IJECI)

VOL: 6
ISSUE: 2 Year 2022

Email ID: ijeci@lgu.edu.pk

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

**LGU International Journal for Electronic Crime Investigation**
Volume 6(2) Year (2022)

## SCOPE OF THE JOURNAL

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

## SUBMISSION OF ARTICLES

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

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

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

**LGU International Journal for Electronic Crime Investigation**
Volume 6(2) Year (2022)

## CONTENTS

**LGU International Journal for Electronic Crime Investigation**
Volume 6(2) Year (2022)

# Virtual Crimes of the Virtual World will Affect us in Future

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

The world keeps on changing. We are continuously innovating and at times creating new threats, challenges, and difficulties for ourselves and the generations to come. Creation of Metaverse will bring us new ways of communicating and new worlds to interact and live in, and probably transform our lives as internet did in the past.

The term metaverse was first coined in 1992 by the author Neal Stephenson in his science fiction novel Snow Crash. Just as the metaverse was science fiction in 1992, today a 'real' metaverse still does not yet exist. The metaverse is often described as a hypothetical iteration of the internet as a single, universal virtual world that presents the user with an immersive experience that feels 'real', usually using a headset. In its very recent definition, it can blur the lines between the physical and virtual world to create a single blended, extended, or mixed reality. As a result, the metaverse is now just focused on virtual reality (VR), but is increasingly being defined in terms of augmented reality (AR) or extended or mixed reality (XR).

Metaverse is a concept on online and persistent 3-D software which creates virtual workspace for each user in which the users are introduced to a virtual life in a virtual universe. The users can live a "second life" where they can buy, sell, meet, socialize, invest etc. and are able to live a second virtual life.

With the recent launch of Meta's platform Horizon Worlds in France and Spain the company is bringing its immersive world or metaverse experience to Europe. When Mark Zuckerberg announced3 in October 2021 that Facebook would now be called Meta, it brought the concept of the metaverse to the public's attention. Google, Microsoft and many others are also making big investments in this technology.

In visions like that of Meta, the metaverse is the evolution of internet, or an embodied internet. Other visions include immersive offline experiences that enable users to experience a different reality, or a combination of the physical and virtual world in a type of mixed reality. An important factor in this is the idea of so-called 'digital twins', which provide a model of offline entities that digitally represent them as accurately as possible, often providing real-time information from sensors. This will allow further integration of the virtual and physical worlds by representing the latter in real-time in the former, autonomously. Thus, integration of the physical and virtual worlds goes both ways, blending both worlds. Examples of this are Seoul's recent announcement to provide many of its access to public services via metaverse is one such example. Even entire countries, such as Singapore, are investing heavily in providing digital twins. An instance of avatar work can be found at a café in Tokyo, where paralyzed people control robot waiters remotely. The waiter can see the café and the people in it through the robot and control it to wait the tables and start a conversation. This enables people to do work they otherwise could not do by using a physical avatar.

According to an estimate published by Europol, it is expected that the total turnover of metaverse will reach 1.6 trillion euros by 2030 and 25% of the population will be spending one hour daily on metaverse.

Despite being in its early stage, the emergence of Metaverse has the potential to be a complete game changer for societies across the world, including for crime and law enforcement.

With the combination of block chain, web3 and NFT technologies, Metaverse will inevitably impact existing criminal threats like crimes

against children and fraud, and generate new forms of crime.

As the Metaverse grows in popularity, the list of crimes will only expand, in some cases defying imagination:

According to a study published by Interpol, some of the crimes which are expected to increase are as follows:

- Money Laundering
- Data Theft
- Child Grooming and Child Sexual Exploitation
- Cyber Attacks in and from Metaverse
- Cyber Physical Attacks
- Financial fraud, social engineering and scams
- Counter feinting and copyright infringements
- Terrorism recruitment and training
- The Darkverse

Are we ready to tackle this probable increase in crimes.

There are new challenges arising for the law enforcement agencies with the advancement in metaverse, which are to be addressed:

- Managing and establishing the authenticity of digital identities in the Metaverse will be a challenge for individuals and institutions, including law enforcement.
- The volume of data collected by the firms operating the Metaverse will magnify the challenge to data protection, privacy, ethics and human rights, with implications for cross-border information exchange as well as building regulatory framework to ensure secure-by-design user experiences.
- Interoperability - the ability to unify economics, avatars, and systems across different virtual worlds - is key to the concept of the Metaverse but will likely present issues for industry leaders/consortiums and regulators.
- Edward Snowden posted on Twitter, outlining that people should not forget that "in five years Zuckerburg gonna own your eyeballs and pause the ads every time you blink." Measures will have to be taken to ensure the safety of users online and offline. This could range from agreeing to certain technical standards to raising awareness about security risks, digital hygiene and «VR Hangover».
- Since currently many parts of the world lack reliable broadband, hardware and/or digital skills needed to access the Metaverse, accessibility and inclusiveness are sure to emerge as key future issues.
- As law enforcement cannot police without legislation, there will be an urgent need for laws that criminalize acts that cause harm in or through the Metaverse. Such efforts may also include efforts to regulate the use and transactions of virtual assets, given their significant role in the Metaverse.

At a session of the 90$^{th}$ general assembly of Interpol, it announced the establishment of first metaverse fully designed for the law enforcement worldwide.

Pakistani law enforcement agencies are in dire need to increase their skills, while other law enforcement agencies are preparing for future cybercrimes, we are still struggling with the existing incidents in the country. Government should develop capacity building programs with the help of public private partnership and support them with sufficient up to date infrastructure. Till then we will remain struggling with various types of cybercrimes and the burden of unsolved cases will keep on growing. May be its time to take combating cybercrimes seriously in Pakistan.

Shairoze *et al.LGU (IJECI)* 2022

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

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 6 issue 2 Year 2022

# A Review of Cyber Security and Cyber-Attacks – What to Know?

**Muhammad Shairoze Malik**
School of Electrical engineering and computer Sciences, National University of Science and Technology, Islamabad.

## Abstract

In this era, human activities have seen a shift and our majority activities including social, cultural, economic and even governmental and NGOs are being done in the cyberspace, especially during and after the crisis of corona pandemic. Due to this shift in communication culture, many individuals and organizations including governments have to face cyber-attacks. Due to heavy reliance on technology and little awareness, defending against cyber-attacks is very challenging. Cyber attacks are usually conducted with the goal of harming an organization or individual financially or these attacks may also be motivated for political or military purposes. Viruses, malwares, ransomwares, denial-of-service and phishing attacks are some of the examples. To protect themselves, organizations employ variety of strategies to mitigate or prevent the threat of these attacks. To prevent and mitigate cyber-attacks, researchers and professionals have devised a number of techniques. This paper is written to thoroughly study and analyze these various approaches and proposed cybersecurity standards, and also to look into the problems, limitations and strengths of these techniques. Fundamental concepts of cyber-attacks and cyber security are discussed along with the current advancements and upcoming trends in security of cyber space. Such a comprehensive review paper would be highly beneficial.

**Keywords:** Cyber Security, Cyber-Attacks, Information Technology, Key Management, Emerging Trends

## 1. Introduction

Internet has become an essential part of our daily lives for the more than two decades now. Due to the technological enhancements and low prices, the internet facility has seen a big boost in its availability, performance and uses. More than 3 billion users are connected to internet now worldwide [1]. Due to e-commerce and other activities, billions of dollars are generated by the global network of internet which has now become a significant portion of global economy [2]. Currently, the majority activities including social, cultural, economic and even governmental and NGOs are being done in the cyberspace [3]. Cyber space has become a center piece in controlling

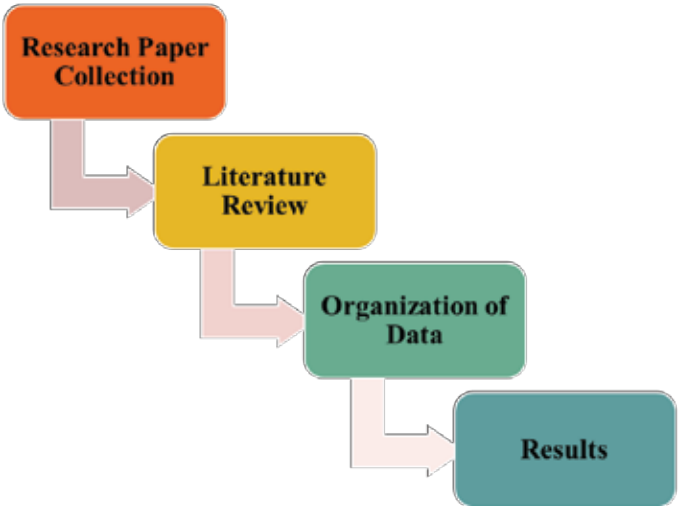
and sharing important and sensitive information around the world [4]. Cyber space has seen a significant increase in activates and financial transactions, through social media and other websites, a significant portion of people's daily life and activities are spent in cyber space as well [5]. A country's GDP (Gross Domestic Product) now has a significant percentage through online companies like e-commerce or freelancing and cyberspace indicators are showing that this percentage is on the rise. These days' cyber space is linked to income and success of a significant portion of people globally [6]. In other words, several components of social life are connected to cyber space and any problem that arise in this space like insecurity or instability will have a direct effect on various areas of social life in real world [7]. All this adds to the problems and challenges for the users and organization which are working in online industry. Low cost to use, anonymity and lack of knowledge about cyber threats have resulted in a rise in cybercrimes either conducted against individuals or organizations by malicious groups or individuals equipped with proper knowledge. Cyber warfare, cyber terrorism, cyber bullying, and cyber espionage are some examples of cybercrimes [8]. All this leads to a very dangerous situation for national security as cybercrimes are not like traditional security threats where the threat actors are usually out in the open [9]. Specialist and analyst have been debating the potential of cyber-attacks on national security for decades [10]. There are numerous incidents of widespread physical and economic damage due to cyber-attacks like an attack on the banking system or virus to disrupt stock market activities or disruption to supply of power by injecting incorrect commands in system or disruption to air traffic control system can cause air accidents, all these cause countries to shut down its operations and lead to security issues [11] [12]. Experts struggle to cope with the cyber-attacks due to a large number of attack vectors across various technologies. It also becomes difficult to enact proper laws and mitigation strategies unless countries have a clear definition of cyber-attacks which are acknowledged by international community [13]. As a result, the question arises [14] as to;

- What constitutes a cyber-attack?
- What its feature are?
- If any attack occurs in cyber space can it be regarded as a crime in its proper definition.

The availability of proper definitions and categorization of cyber-attacks can no doubt help legal fraternity to establish proper laws and punishments. Without a clear picture and lack of knowledge about severity of cyber-attacks, it leads to diversity in interpretations and practices which eventually leads to sometimes contradicting legal results [15] [16]. Therefore, the importance of fundamental knowledge of cyber-attacks, there working and analysis is of paramount importance and it necessitates extensive and continuous research. The foundational knowledge of cyber-attacks is discussed in this paper, followed by an analysis of mitigation techniques and categorization of cyber-attacks. Current definitions are analyzed from the perspective of global specialists and organizations. In the end conclusion of paper is provided.

## 2. Methodology

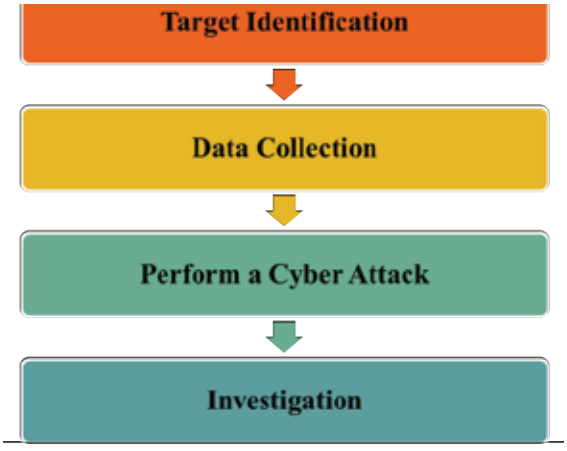
The methodology used in this research paper is explained in the below diagram:




(Figure 1: Methodology)

## 3. Fundamental Concepts

Cyber assaults are part of a larger context than what is generally referred to as information operations. Electronic warfare, psychology, computer networks, military tricks and security operations, and other major capabilities, combined with special support and related capabilities, are used extensively in information operations to infiltrate, hijack or stop human decision-making [17]. The steps of a cyber-attack can be depicted as shown in Figure 2.




(Figure 2: Anatomy of a Cyber-Attack.)

Computer network operations, according to the USNM cyberspace operations strategy, include attack, defense, and exploit enablement [18]. The latter differs from cyber assaults and cyber defenses as it main focus is on acquiring and analyzing information and not on damaging the network, it can act as a preparation phase for an attack [19]. Such activities can also be conducted out in order to disseminate information and propaganda [20]. To steal important computer data, computer-network activities can also be undertaken. Wire taps and key loggers are effective tools for cyber espionage in this situation [21]. External users can access software through trap doors at any moment without the computer user's awareness. A sniffer is a program used to steal usernames and passwords [22]. Table 1 summarizes the fundamental concepts and definitions of cyber-space.

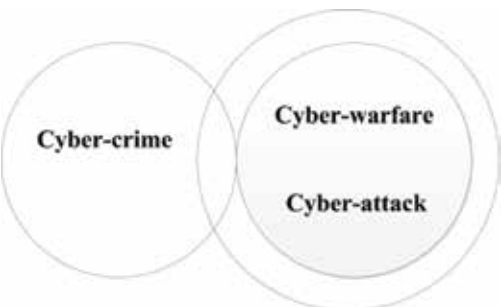
**Table 1:** Fundamental concepts and basic definitions of cyberspace [12] [19] [29] [30].

| *Concept* | *Definition* |
|---|---|
| ***Cyberspace*** | Cyberspace is an interconnected network of all the communication devices worldwide including computer systems, servers, IT infrastructure, information exchange and the interaction between technology and humans for information processing, exchange, storage, retrieval and utilization. |
| ***Cyber capital*** | Sensitive infrastructure, critical network systems, critical information, or citizens of a country. |
| ***Cyber vulnerability*** | A flaw in security program, or internal control, or in the implementation of cyber asset, which may be exploited or triggered by an internal or foreign adversary to perform cyber-attack. |
| ***Cyber-threats*** | Any incident that has the potential to disrupt cyber space such as illegal access, disclosure, destruction or manipulation of information, and/or blockage/disruption of service delivery. |
| ***Cyber-threat-level*** | Cyber threat levels can be distinguished as: individual, provisional, institutional, critical infrastructure, national and international. |
| ***Cyber threats probability*** | Probability of cyber threats can be categorized as: imminent, probable, unlikely, very unlikely. |
| ***Cyber threats intensity*** | Intensity of cyber threats can be classified as disaster (very high), crisis (high), major security incident (moderate), normal security incident (low) and small security incident (very low). |
| ***Cyber attack*** | A cyber-attack is defined as any illegal cyber action targeted at breaking cyber asset security policies and inflicting harm, disruption, or interruption of services or access to information on cyber assets in that jurisdiction. A cyber-attack is also defined as the intentional use of cyber weapons against information systems that results in a cyber-incident. |
| ***Cyber weapon*** | Cyber weapons are systems that are intended and built to interfere with the structure or functioning of other cyber systems. Botnets, logic bombs, network exploits, malware, and traffic creation systems are examples of technologies used to prevent service attacks and distributed services. |
| ***Cyber-warfare*** | It is the highest degree and most intricate cyber-attacks carried out against various nations' cyber interests and has the most devastating implications. |
| ***Cyber warfare origin*** | An aggressor state or group under an aggressor state organization control or abandons cyber power and cyber weapons. |
| ***Cyber defense*** | Deterrence, prevention, preventive, quick detection, effective, and deterrent reaction to any cyber assault using all unarmed cyber and non-cyber facilities of a nation |
| ***Cyber-biome*** | The construction of native and dynamic cyber environments that assist a nation in numerous domains is referred to as a cyber-biome. |
| ***Computer Virus*** | A computer virus is a piece of code that replicates itself and spreads to other programs, causing the programs to malfunction. NIMDA, SLAMMER, and SASSER are several well-known viruses. |
| ***Computer Hacker*** | A person who gains an unauthorized access to a system or information in order to read, copy, delete, replace or destroy data. |

Cyberwarfare may have the following implications [23] [5] [24]:

- Overthrow the governing system or constitute a catastrophic danger to national security;
- Begin traditional warfare at the same time to assist the start of physical combat;
- Causing catastrophic damage or harm to the country's image on a global scale;
- Causing severe disruption or harm to the country's political and economic connections;
- Internal turmoil; mass casualties or a threat to public health and safety;
- State administration is being disrupted on a large scale;
- Undermining public trust or national, religious and ethnic beliefs;
- Serious economic harm to the country;
- Widespread interruption or disruption of cyber systems.

In addition to these, five scenarios may also be considered for cyber warfare: (1) governments sponsored cyber-attacks to acquire information for future attacks, (2) cyber-attacks intended at laying the framework for any disturbance or public movement, and (3) cyber-attacks aiming at causing harm. In cyberattacks that impair equipment and aid physical assaults, (4) cyberattacks that supplement physical attacks, and (5) cyberattacks with the ultimate purpose of widespread devastation or disruption (cyber warfare) [25]. Encryption is one sort of cyber assault. Encryption is a reversible technique of encrypting data that necessitates the use of a key to decrypt. Encryption can be used in tandem with encryption to give an additional degree of secrecy [26]. Encryption is the practice and study of encrypting and decrypting data such that it can only be decoded by a certain individual. The cryptosystem is the system used to encrypt and decode data [27]. Encryption is a strong tool for securing sensitive and private information from strangers and criminals, as well as concealing unwanted behavior from law enforcement. Cryptographic techniques require continual integration to reduce vulnerabilities as computers get faster and failover solutions become more secure [28]. It is important to note that there is a distinction between cybercrime, cyberwarfare, and cyberattack in general. Figure 3 and Table 2 demonstrate the conceptual contrast between cybercrime, cyberwarfare, and cyberattack.




(Figure 3: Conceptual contrast between cybercrime, cyberwarfare, and cyberattack)

**Table 2:** Conceptual contrast between cybercrime, cyberwarfare, and cyberattack [31] [32].

| *Type* | *Features* |
|---|---|
| *Cyber_Crime* | Actions taken in cyber space by an individual or organization usually by non-governmental attackers in violation of criminal law and is carried out through the help of computer system. |
| *Cyber_Attack* | To disrupt of destroy the working operation of a computer network. |
| *Cyber_Warfare* | The warfare conducted between nations for political or security purposes in the cyberspace and is similar or more deadly to an armed attack. |

### 3.1 Specialists' Point of View

Experts in the legal and technological disciplines have devised a variety of definitions of cyberattack, the most notable of which are as follows:

According to Richard Clark, a cyberattack is an activity taken by a state to enter a computer or computer network in one or more nations with the intent of causing harm or destruction [33]. In the examination and critique of this definition, it can be stated that the perpetrator of the assault, the goal of the attack, and the intent of the attack are three factors as the standard, without taking into account the type of harm [34]. In addition, only the state is often recognized as the perpetrator of an assault if the attack is begun by a person in a context and geographic region (the cyberspace of a state-controlled network) under the control and jurisdiction of a state. If NGOs and private organizations conduct action against foreign nations, they are mainly beyond the scope of the preceding description and are not covered, leaving a vacuum in the legal coverage of such actions. Given this position, it is reasonable to conclude that the above definition is essentially inadequate, since it excludes the majority of assaults carried out by private and non-governmental organizations, resulting in a void [31].
Michael Hayden: Any purposeful effort to destroy or disrupt another country's computer network [35]. Obviously, this term is also quite broad and makes no distinction between cybercrime, cyberattack, and cyberwarfare, and the borders between their detection are blurred, and the lack of this distinction will undoubtedly affect critics and policymakers. The wide framework of the norms of war allows for unfettered internet, which will undoubtedly have harmful and negative repercussions for the expansion of war and the belligerence of states [36]. So, the preceding definition's generality is also its fundamental flaw, resulting in a lack of luck. In contrast to the first definition, which confined the perpetrator of an assault to a government aggressor, this term is broad, simple to interpret, and, as previously said, may be harmful, have bad consequences, and lead to international conflicts. Relations are tumultuous, and they eventually constitute a danger to international peace [37].

Martin Libicki: A digital assault on a computer system causes the targeted computer system to look normal while creating and sending out erroneous replies [38]. This definition of a cyber-assault effectively eliminates a wide variety of possible dangers to the national security of nations whose cyber infrastructure has been targeted but has not yet reached the degree and threshold of substantial attack. The fact is that these threats can inflict harm to the target country's computer systems and networks. As a result, any definition of cyber assault that excludes the aforementioned is unavoidably inadequate and not necessarily

comprehensive [39] [40].

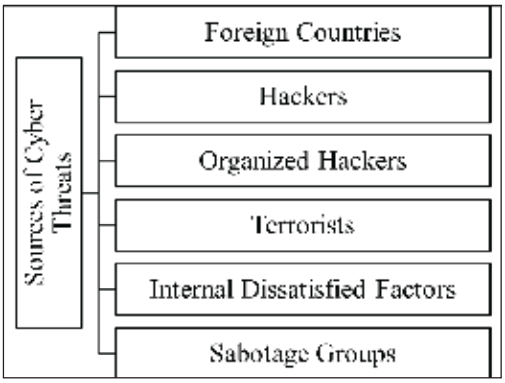
Tallinn Manual Group: A cyber-attack is a malicious or defensive cyber action that causes casualties, property damage, or destruction. The issue of contention with this definition is the produced outcome and effect. According to the source of this definition, a cyber-attack is of the attack type if it results in the outcomes indicated in the definition (i.e., causing bodily and economic harm) [29]. As a result, rather than the attack itself, the main basis for this group's definition is the result-oriented nature of a cyber-attack; such an attack can be described as an attack if it leaves an objective, tangible, violent effect and consequence, while at this stage, the rules of international law in relevant fields and areas (right to resort to duress, the law of war, and the law of international responsibility will be enforceable [41].

## 4. Cyberspace Threats

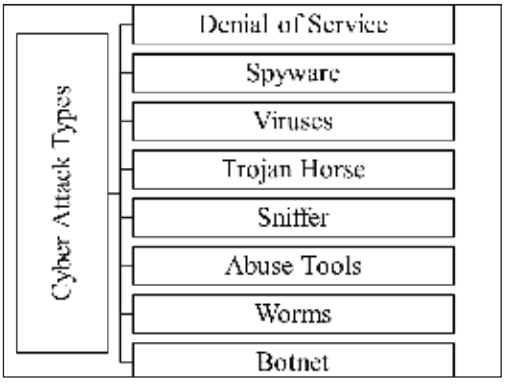
Naturally, the scale of global cyberspace produces overlapping spheres of control for state actors with varying cultural and legal approaches as well as strategic goals [42]. Countries all around the world already rely significantly for communication and control of the real world on cyber space. As a result, cyberspace is progressively influencing state security responsibilities and functions [43]. There is no certainty in the product supply chain process due to worldwide manufacture of hardware and software goods. The network realm is qualitatively distinct due to its scalability. Bombs have a limited physical reach in the most extreme situations; but, the reach of cyber threats is quite vast; hence, we have a method by which we may regulate real-world activities. Cyberspace activities, like many other disciplines of expertise, are controlled by a small number of people. Users are unable to change or control the software and hardware that they utilize. To manage and control cyber warfare there are only few organizations that are capable and it is no secret [44]. Despite the requirement for focus and competence, the scattered structure of the cyber world prohibits a single individual or group of people from gaining total control. Changes in the networking industry are occurring at a rapid pace and are based on the ongoing development of computing and communication technology. This acceleration is aided by network cohesiveness. Every transition ushers in a new period of sensitivity and responsiveness. Cyberspace, far from being stagnant throughout [45], is nearly dynamic. The distribution of cyber assets is similar to all sorts of organizations, ranging from closed and government-controlled systems to those owned and managed by society's private sector, each with various resources and facilities, as well as varied skills and concerns [46]. Because of the nature of cyberspace, there is currently no technical capability to confidently attribute actions to people, groups, or organizations. External threats, internal threats, threats in the supply chain of products and services, and risks owing to poor operational capabilities of local forces are the primary dangers in cyberspace [47]. Some intelligence collecting and espionage actions are carried out by foreign intelligence services using cyber technologies. Many similar examples have been documented throughout the world as a result of the exploitation and disruption of national information infrastructure, such as computer systems, Internet information networks, and processors

and controllers implanted in critical sectors. Another source of assaults is groups who target network systems for profit, and the number of attacks by these groups is growing [48]. In addition, other organizations (hackers) occasionally infiltrate the network to express themselves. In the current state of affairs, it is feasible to enter the network with minimum knowledge and abilities by obtaining the essential applications and protocols from the Internet and utilizing them for other sites. Simultaneously, another politically motivated organization known as hacktivism launched attacks on major online pages or email providers. These organizations often raise the burden on email providers and distribute their political messages through website infiltration [49]. Dissatisfied agents within an organization, on the other hand, are a key source of cybercrime, and these agents do not require a great deal of understanding about cyberattacks; since their target system awareness typically provides unlimited access to the system or takes the company's information. Terrorists are another source of risks because they aim to damage, disable, or deliberately exploit vital infrastructure in order to endanger national security, create large losses, harm national economies, and disrupt public attitude and confidence [50]. Figure 4 depicts the origins of cyber-attacks.

Denial of service, logic bombs, abuse tools, sniffers, Trojans, viruses, worms, spam, and botnets are the most common cyber assault tactics. Figure 5 depicts many forms of cyber-attacks. The authorized user's access to the system is denied in a denial of service attack, and vice versa. In fact, the attacker eventually immerses the target machine in numerous messages and disrupts legal data flow. This stops any system from connecting to the Internet or interacting with other systems [51]. They attack from a huge number of distributed systems at the same time in another strategy known as wide denial of service. This is commonly accomplished by spreading worms across numerous computers in order to assault the target. The public can use abusive tools to find and penetrate weaknesses in networks with differing skill levels. Another sort of attack is logic bombs, in which programmers add code into a software that automatically conducts damaging operations whenever a specified event happens [52] [53]. A sniffer is a software that listens in on routing information and searches for particular information such as passwords by inspecting each packet in the data stream [54]. Trojans conceal deadly code and frequently masquerade as beneficial applications that victims are prepared to use [55]. Viruses also taint system files, mainly utilities, by introducing copies of themselves into these files. These versions execute by loading the infected file into memory, allowing the virus to infect subsequent files. Viruses, unlike worms, require human assistance to propagate. A worm, on the other hand, is a self-replicating system software that copies itself from one computer to another on a network [56]. Finally, a botnet is a network of compromised remote control devices that are used to distribute malware, coordinate assaults, spam, and steal data. Botnets are often deployed discreetly on target computers, allowing unauthorized individuals to remotely manipulate the target system in order to achieve their harmful objectives. Botnets are frequently referred to as "electronic troops" [57].




(Figure 4: Cyber threat sources)



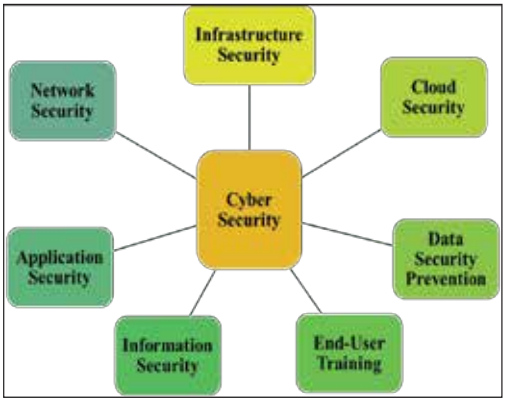

(Figure 5: Cyber-attack types.)

Qiu and his colleagues investigated the impact and danger of cybersecurity in a WAMS-based FFR (fractional flow reserve) control using a unique scale CNN to interpret faked data from two scales [58]. They are also researching a cybersecurity defensive strategy for FFR systems based on time and frequency. The results reveal that true synchro phasor data is more accurate and robust. Based on knowledge-based hidden Makrove modelling, Lee and his colleagues created a way to unify the cyberattack recovery process [59]. They also investigated a safe state approximation approach based on the updated HMM. A case study demonstrates the efficacy of the presented strategy. Zhang and Malacaria developed a cybersecurity decision support system to help organizations choose the appropriate security combination to fight against multi-stage assaults [60]. To identify ongoing threats, the system includes LM-powered online and preventative improvements. They discovered a Bayesian STACKELBERG game of selecting efficient solutions online. Kim and his colleagues investigated NPP for cyberattack likelihood factors [61]. Furthermore, AHP and FA are used to quantify the comparative importance of NPP likelihood factors. They discovered that support for South Korea's approach to cybersecurity was associated with a stronger preference for execution. According to Tosun, the cyberattack had an immediate detrimental impact on the company's reputation. Furthermore, financial markets have increased in a rebound drop in response to corporate security breaches. Furthermore, transaction rates have risen as a result of selling pressure and improved liquidity. R&D and dividends fall with time, whereas target firms continue to pay CEOs [62].

## 5. Mitigation Techniques – Cyber Security

Cybersecurity is a critical concern in the infrastructure of any business and organization. In brief, a cybersecurity-based firm or organization can gain high status and numerous accomplishments as a consequence of the company's capacity to secure private and consumer data from rivals. Customers' and individuals' competitors, as well as organizations, are abusive. In order to thrive and flourish, a firm or organization must first provide the highest available security [63]. Cybersecurity is taking real steps to secure information,

networks, and data from internal and external threats. Cybersecurity experts safeguard networks, servers, intranets, and computer systems. Cybersecurity guarantees that only those who are permitted have access to this information [12]. Understanding the different forms of cybersecurity is essential for effective defense. Figure 6 depicts the many forms of cybersecurity.




(Figure 6: Types of cyber security)

**Network-Security:** To safeguards computer networks against viruses and hackers. Cybersecurity refers to a collection of solutions that allow firms to protect computer networks against hackers, organized attacks, and viruses [64].

**Application Security:** The use of software like antivirus applications, encryption, and firewalls or the use of hardware devices to secure systems from threats that may interfere with application development [65].

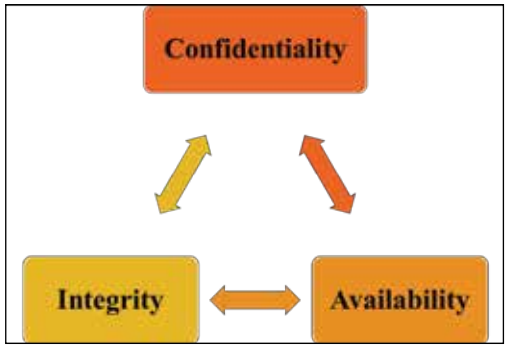
**Information Security:** The digital data must be protected from misuse, disclosure, unauthorized access, unlawful change, and deletion [66].

**Operational security:** The methods and decisions taken to regulate and secure data are referred to as operational security. For example, user privileges when connecting to a network, or processes that determine when and where information can be kept or exchanged [66].

**Cloud Security:** Cloud security is the process of protecting information/data stored in the cloud through tools and monitoring it in order to remove the possibility of on-site assaults [67].

**User training:** Individuals are the unexpected parts of cybersecurity. A virus can be inadvertently infected into a security system by anyone. Teaching employees to not to connect anonymous USB drives, to remove suspicious attachments in emails and other crucial concerns should be part of every corporate security policy [67].

Cybercrimes can be any actions that are unlawful and are performed to compromise a system, device or network. It can be categorized in two types: crimes that target systems and crimes in which systems operate inadvertently. Table 3 depicts the strategies most typically employed by cybercriminals. Any organization's security must have three principles: Confidentiality, Integrity, and Availability. These three principles are known as the CIA Triad and they have been the norm for system security from the early days of computing (see Figure 7) [68].




(Figure 7: CIA Triad)

**Table 3:** Strategies most typically employed by cybercriminals.

| *Method Name* | *Description* |
|---|---|
| ***Denial_of_Service (DOS)*** | To disrupt the services of a computer system by exhausting all the network resources of the system. As a result system users can get access to it [19]. |
| ***Man_in_the_Middle*** | To eavesdrop the communication between victim and server by sniffing the network traffic. Attacker can even change data packets [72]. |
| ***Computer Malware*** | To infect victims using computer viruses or worms [36]. |
| ***Phishing*** | To make user disclose his personal or organizations confidential information by using physiological techniques using emails or other platforms [50]. |

According to the Confidentiality concept, only those who have proper authorization can have access to sensitive information and can make use of sensitive functionalities of an organization. According to the Integrity concept, only authorized personnel are permitted to edit, remove or delete sensitive information and functions. According to the Availability concept, systems, services, and data must be made available on demand in accordance with specified specifications based on SLA service levels [69]. The greatest cybersecurity procedures go above and beyond the aforementioned criteria. This basic protection can be circumvented by any competent hacker. As a company grows in size, cybersecurity gets increasingly complex. Another cybersecurity restriction is coping with the increasing number of persons participating in the flow of virtual and real-world data. The shortage of skilled vocations to do the work is a significant barrier in cybersecurity. Many are at the bottom end of the cybersecurity vision, with general abilities. Coverage of cyberspace is a big topic. In the next essay, we'll go through the many sorts of cybersecurity. A complete approach takes into account all of these factors and does not overlook any of them [70]. The world's key infrastructure is a hybrid of cyber and physical components. This amazing building provides us with several advantages. Deploying online systems, on the other hand, introduces additional vulnerabilities for hackers and cyberattacks. Organizational decision-makers must priorities how an assault impacts their performance. Some of the most talented new hackers regard web application security as the weakest link in the chain of attack on corporations. This reduces the amount of labor required to hack and infiltrate the information. Cybersecurity is getting increasingly sophisticated. Businesses must have a "security perspective" on how cybersecurity works. Because of heightened security dangers, investments in cybersecurity systems and services are expanding. McAfee, Cisco, and Trend Micro are three businesses that are involved in this space [71].

## 5.1 Cyber-Security Policy

Over time, the network boosts community production and effectively distributes knowledge. No matter whatever application or industrial network is used, the goal is to increase output. The rapid movement of data to cyberspace primarily undermines the entire system's security. Security metrics are frequently in direct opposition with progress for technical experts enhancing production, since preventative measures decrease, ban, or delay user access, consume metrics that indicate impor-

tant system resources, and respond to management concerns [73]. The term "policy" refers to rules and regulations for the dissemination of information, data protection objectives for the commercial sector, and system operational policies for technological controls in a number of domains relevant to cybersecurity. However, the word cybersecurity policy is used for a distinct reason in this field. There is no definitive definition of cybersecurity policy, as there is for the word "cyberspace," but when used as an adjective in the policy area, it alludes to a common notion [74].

Cybersecurity rules are recognized by the regulatory framework and explicitly applied to the regulator's relevant areas. The components of security policies differ depending on the policy scope [75]. National cybersecurity policy, for example, applies to all citizens and maybe international businesspeople operating in the industry, but corporate cybersecurity only applies to personnel who are hired or have legal contracts and are required to manage their behavior toward the organization. It is not realistic to expect resource suppliers that are totally dependent on one client to comply with client security standards unless a written contract is in existence [76]. National security objectives are not the same as business security objectives. The implementing agency is in charge of interpreting and registering the policy, and the regulatory committee and appropriate authorities are in charge of approving it. However, in most businesses, a centralized security department is in charge of cybersecurity policies, standards, and solutions. The enterprise security unit's standards and solutions serve as a reference for legislation. When security becomes a high concern for a company, cybersecurity rules are published by various internal units of the Common Component Wing. These shared components can occasionally detect policy discrepancies caused by attempting to implement these concerns concurrently [38].

The country's cyber policy is now integrated into its national security strategy. Indeed, policies are formed and disseminated in papers and lectures via discussions and debates of many points of view. Rules and regulations have nothing to do with policies. Laws, agreements, and guidelines, at best, offer a meaningful and logical policy. Cybersecurity enforcement orders, rules, and regulations, on the other hand, can be issued without the creation of a cybersecurity policy [77].

Different sectors are required to respect the norms in a corporate environment owing to the threat of fines, which will remain until the violating sector closes. For example, code HR, civil, or costing policies such that any violation of notification rules results in the closure of the relevant department. Middle managers are required to implement communication policies into departmental operations and generate metrics at the departmental level to measure policy compliance, as well as to assist procedures such as hiring personnel or submitting costs. Any sort of organizational division has governance limits in the public sector [78]. There are instances in which different aspects of information categorization are significantly weighted, but the corporate security policy supplied by the CEO applies to the whole firm, but the security policy released by the CEO is confined to the domain. Technicians should apply. One of the most recent organizational-wide improvements has been the appointment of senior data security managers or senior

managers in charge of choosing various aspects of an organization's security posture. Also, one of the disadvantages of corporate cybersecurity policy against HR/legal policy is that it is delegated to middle management. When the danger of disclosure of sensitive information is considerable, cybersecurity regulations may demand that information not be delivered without a comprehensive review of the recipient's capacity to preserve the security of the information [79]. The policy defers data risk assessment to managers who may seek to save money by outsourcing information flow to the office and utilizing personnel outside the office for information analysis. Perhaps the same boss wishes to avoid inspection in order to reduce expenditures. This circumstance may be the consequence of a miscalculation of non-security professionals' information obligations, or it may be that the culture of the organization involved accepts the risk. In every scenario, work division is critical. These circumstances are exacerbated by the fact that cybersecurity measurements have not yet developed as accounting or HR metrics.

## 6. Conclusion

Cyber space and associated technologies are an important sources of power for current generation. The asymmetry of cyberspace along with anonymity and lack of security measures plus the low cost to access internet creates a situation of power dissipation. Because of which along with the measure taken at governmental level, individuals and private organizations have to also put in effort against the malicious actors in cyber space. Cyber-attacks jeopardize the national security, and its impact may be measured in various ways. The first is that the national security can no longer be defined solely in terms of internal and external boundaries; technological advancements in people's daily life pose a threat to national security as well due to interlinked services. The second is the removal of geographical boundaries of cyber threats; military threats used to have a definite geographical location with which it was easy to identify security threats but that's not the case in terms of cyber space. The third factor is the varying level of vulnerabilities brought by cyber threats; the attacks and intermittent, multi-dimensional and extremely damaging due to their link with the critical infrastructure and networks. Fourth is that the traditional tools used by security agencies for the mitigation and containment of threats are insufficient. Governments alone cannot cope with all these variables. Effective bilateral collaboration between governments and the business sector is mutually beneficial in dealing with these threats. Fifth, as seen in the preceding point, cyber risks are not restricted to governments, and people and businesses are not immune to them. In the end, only with a collective effort and use to proper tools along with adequate knowledge can the threats of cyber-attacks in cyber space be minimized.

## 7. References

[1] Tan, Sen, Peilin Xie, Josep M. Guerrero, Juan C. Vasquez, Yunlu Li, and Xifeng Guo. "Attack Detection Design for Dc Microgrid Using Eigenvalue Assignment Approach." *Energy Reports*, ICPE 2020-The International Conference on Power Engineering, 7 (April 1, 2021): 469–76.

[2] Judge, Malik Ali, Awais Manzoor,

Carsten Maple, Joel JPC Rodrigues, and Saif ul Islam. "Price-Based Demand Response for Household Load Management with Interval Uncertainty." *Energy Reports* 7 (2021): 8493–8504.

[3] Aghajani, Gholamreza, and Noradin Ghadimi. "Multi-Objective Energy Management in a Micro-Grid." *Energy Reports* 4 (November 1, 2018): 218–25.

[4] Akhavan-Hejazi, Hossein, and Hamed Mohsenian-Rad. "Power Systems Big Data Analytics: An Assessment of Paradigm Shift Barriers and Prospects." *Energy Reports* 4 (November 1, 2018): 91–100.

[5] Priyadarshini, Ishaani, Raghvendra Kumar, Rohit Sharma, Pradeep Kumar Singh, and Suresh Chandra Satapathy. "Identifying Cyber Insecurities in Trustworthy Space and Energy Sector for Smart Grids." *Computers & Electrical Engineering* 93 (July 1, 2021): 107204. https://doi.org/10.1016/j.compeleceng.2021.107204.

[6] Amir, Maral, and Tony Givargis. "Pareto Optimal Design Space Exploration of Cyber-Physical Systems." *Internet of Things* 12 (December 1, 2020): 100308.

[7] Li, Nianyu, Christos Tsigkanos, Zhi Jin, Zhenjiang Hu, and Carlo Ghezzi. "Early Validation of Cyber–Physical Space Systems via Multi-Concerns Integration." *Journal of Systems and Software* 170 (December 1, 2020):

[8] Niraja, K. S., and Sabbineni Srinivasa Rao. "A Hybrid Algorithm Design for near Real Time Detection Cyber Attacks from Compromised Devices to Enhance IoT Security." *Materials Today: Proceedings*, 2021.

[9] Sarker, Iqbal H. "CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks." *Internet of Things* 14 (June 1, 2021): 100393.

[10] Shin, Jinsoo, Jong-Gyun Choi, Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Jun-Young Son. "Application of STPA-SafeSec for a Cyber-Attack Impact Analysis of NPPs with a Condensate Water System Test-Bed." *Nuclear Engineering and Technology* 53, no. 10 (2021): 3319–26.

[11] Snehi, Manish, and Abhinav Bhandari. "Vulnerability Retrospection of Security Solutions for Software-Defined Cyber–Physical System against DDoS and IoT-DDoS Attacks." *Computer Science Review* 40 (May 1, 2021): 100371.

[12] Ahmed Jamal, Alshaibi, Al-Ani Mustafa Majid, Anton Konev, Tatiana Kosachenko, and Alexander Shelupanov. "A Review on Security Analysis of Cyber Physical Systems Using Machine Learning." *Materials Today: Proceedings*, July 8, 2021.

[13] Cao, Jie, Da Ding, Jinliang Liu, Engang Tian, Songlin Hu, and Xiangpeng Xie. "Hybrid-Triggered-Based Security Controller Design for Networked Control System under Multiple Cyber Attacks." *Information Sciences* 548 (February 16, 2021): 69–84.

[14] Gupta Bhol, Seema, JR Mohanty, and

Prasant Kumar Pattnaik. "Taxonomy of Cyber Security Metrics to Measure Strength of Cyber Security." *Materials Today: Proceedings*, June 24, 2021.

[15] Furnell, Steven, and Jayesh Navin Shah. "Home Working and Cyber Security – an Outbreak of Unpreparedness?" *Computer Fraud & Security* 2020, no. 8 (August 1, 2020): 6–12.

[16] Alhayani, Bilal, Sara Taher Abbas, Dawood Zahi Khutar, and Husam Jasim Mohammed. "Best Ways Computation Intelligent of Face Cyber Attacks." *Materials Today: Proceedings*, March 10, 2021.

[17] "Riskio: A Serious Game for Cyber Security Awareness and Education - ScienceDirect." Accessed March 27, 2022.

[18] Ma, Lei, Ying Zhang, Chunyu Yang, and Linna Zhou. "Security Control for Two-Time-Scale Cyber Physical Systems with Multiple Transmission Channels under DoS Attacks: The Input-to-State Stability." *Journal of the Franklin Institute* 358, no. 12 (August 1, 2021): 6309–25.

[19] Alghamdie, Mohammed. I. "A Novel Study of Preventing the Cyber Security Threats." *Materials Today: Proceedings*, April 23, 2021. https://doi.org/10.1016/-j.matpr.2021.04.078.

[20] Thomson, J. R. "Chapter 3 - Cyber Security, Cyber-Attack and Cyber-Espionage." In *High Integrity Systems and Safety Management in Hazardous Industries*, edited by J. R. Thomson, 45–53. Boston: Butterworth-Heinemann, 2015.

[21] Liu, Xiaoxue, Jiexin Zhang, Peidong Zhu, Qingping Tan, and Wei Yin. "Quantitative Cyber-Physical Security Analysis Methodology for Industrial Control Systems Based on Incomplete Information Bayesian Game." *Computers & Security* 102 (March 1, 2021): 102138.

[22] Karbasi, Ali, and Alireza Farhadi. "A Cyber-Physical System for Building Automation and Control Based on a Distributed MPC with an Efficient Method for Communication." *European Journal of Control* 61 (September 1, 2021): 151–70.

[23] Khan, Shah Khalid, Nirajan Shiwakoti, Peter Stasinopoulos, and Yilun Chen. "Cyber-Attacks in the next-Generation Cars, Mitigation Techniques, Anticipated Readiness and Future Directions." *Accident Analysis & Prevention* 148 (December 1, 2020): 105837.

[24] Mehrpooya, Mehdi, Noradin Ghadimi, Mohammad Marefati, and Sohrab Ali Ghorbanian. "Numerical Investigation of a New Combined Energy System Includes Parabolic Dish Solar Collector, Stirling Engine and Thermoelectric Device." *International Journal of Energy Research* 45, no. 11 (2021): 16436–55.

[25] Alibasic, Armin, Reem Al Junaibi, Zeyar Aung, Wei Lee Woon, and Mohammad Atif Omar. "Cybersecurity for Smart Cities: A Brief Review." In *Data Analytics for Renewable Energy Integration*, edited by Wei Lee Woon, Zeyar Aung, Oliver Kramer, and Stuart Madnick,

22–30. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-50947-1_3.

[26] Sun, Chih-Che, Adam Hahn, and Chen-Ching Liu. "Cyber Security of a Power Grid: State-of-the-Art." *International Journal of Electrical Power & Energy Systems* 99 (July 1, 2018): 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020.

[27] ji, Zuzhen, Shuang-Hua Yang, Yi Cao, Yuchen Wang, Chenchen Zhou, Liang Yue, and Yinqiao Zhang. "Harmonizing Safety and Security Risk Analysis and Prevention in Cyber-Physical Systems." *Process Safety and Environmental Protection* 148 (April 1, 2021): 1279–91. https://doi.org/10.1016/j.psep.2021.03.004.

[28] Zou, Tierui, Arturo S. Bretas, Cody Ruben, Surya C. Dhulipala, and Newton Bretas. "Smart Grids Cyber-Physical Security: Parameter Correction Model against Unbalanced False Data Injection Attacks." *Electric Power Systems Research* 187 (October 1, 2020): 106490. https://doi.org/10.1016/j.epsr.2020.106490.

[29] Bullock, Jane A., George D. Haddow, and Damon P. Coppola. "Chapter 8 - Cybersecurity and Critical Infrastructure Protection." In *Introduction to Homeland Security (Sixth Edition)*, edited by Jane A. Bullock, George D. Haddow, and Damon P. Coppola, 425–97. Butterworth-Heinemann, 2021.

[30] Ashraf, Javed, Marwa Keshk, Nour Moustafa, Mohamed Abdel-Basset, Hasnat Khurshid, Asim D. Bakhshi, and Reham R. Mostafa. "IoTBoT-IDS: A Novel Statistical Learning-Enabled Botnet Detection Framework for Protecting Networks of Smart Cities." *Sustainable Cities and Society* 72 (September 1, 2021): 103041.

[31] Zhang, Ting. "A Comparative Study on Sanction System of Cyber Aider from Perspectives of German and Chinese Criminal Law." *Computer Law & Security Review* 33, no. 1 (February 1, 2017): 98–102.

[32] Dash, Nitu, S. Chakravarty, and Suneeta Satpathy. "An Improved Harmony Search Based Extreme Learning Machine for Intrusion Detection System." *Materials Today: Proceedings*, February 26, 2021.

[33] Motsch, William, Alexander David, Keran Sivalingam, Achim Wagner, and Martin Ruskowski. "Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems." *Procedia Manufacturing*, 30th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2021), 51 (January 1, 2020): 1748–54.

[34] Cao, Yan, Zhiqiu Huang, Changbo Ke, Jian Xie, and Jinyong Wang. "A Topology-Aware Access Control Model for Collaborative Cyber-Physical Spaces: Specification and Verification." *Computers & Security* 87 (November 1, 2019): 101478.

[35] Robinson, Michael, Kevin Jones, and

Helge Janicke. "Cyber Warfare: Issues and Challenges." *Computers & Security* 49 (March 1, 2015): 70–94.

[36] Edgar, Thomas W., and David O. Manz. "Chapter 2 - Science and Cyber Security." In *Research Methods for Cyber Security*, edited by Thomas W. Edgar and David O. Manz, 33–62. Syngress, 2017.

[37] Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. "SCADA Security in the Light of Cyber-Warfare." *Computers & Security* 31, no. 4 (June 1, 2012): 418–36.

[38] Quigley, Kevin, Calvin Burns, and Kristen Stallard. "'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection." *Government Information Quarterly* 32, no. 2 (April 1, 2015): 108–17.

[39] Damon, Evan, Jens Mache, Richard Weiss, Kaleb Ganz, Claire Humbeutel, and Miles Crabill. "Chapter 31 - Cyber Security Education: The Merits of Firewall Exercises." In *Emerging Trends in ICT Security*, edited by Babak Akhgar and Hamid R. Arabnia, 507–16. Boston: Morgan Kaufmann, 2014.0031-1.

[40] "Designing a PID Controller to Control a Fuel Cell Voltage Using the Imperialist Competitive Algorithm - Advances in Science and Technology. Research Journal - Tom Vol. 10, Nr 30 (2016) - BazTech - Yadda." Accessed March 27, 2022.

[41] Chen, Ji-Kang, Ching-Wen Chang, Zhiyou Wang, Li-Chih Wang, and Hsi-Sheng Wei. "Cyber Deviance among Adolescents in Taiwan: Prevalence and Correlates." *Children and Youth Services Review* 126 (July 1, 2021): 106042.

[42] Iqbal, Zafar, and Zahid Anwar. "SCERM—A Novel Framework for Automated Management of Cyber Threat Response Activities." *Future Generation Computer Systems* 108 (July 1, 2020): 687–708.

[43] Zhao, Jun, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. "TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data." *Computers & Security* 95 (August 1, 2020): 101867.

[44] Zhang, Xiaoyu, Maochao Xu, Gaofeng Da, and Peng Zhao. "Ensuring Confidentiality and Availability of Sensitive Data over a Network System under Cyber Threats." *Reliability Engineering & System Safety* 214 (October 1, 2021): 107697.

[45] Varga, Stefan, Joel Brynielsson, and Ulrik Franke. "Cyber-Threat Perception and Risk Management in the Swedish Financial Sector." *Computers & Security* 105 (June 1, 2021): 102239.

[46] "Control-Theory Based Security Control of Cyber-Physical Power System under Multiple Cyber-Attacks within Unified Model Framework - ScienceDirect." Accessed March 27, 2022.

[47] Al-Ghamdi, Mohammed I. "Effects of

Knowledge of Cyber Security on Prevention of Attacks." *Materials Today: Proceedings*, April 27, 2021.

[48] Beechey, Matthew, Konstantinos G. Kyriakopoulos, and Sangarapillai Lambotharan. "Evidential Classification and Feature Selection for Cyber-Threat Hunting." *Knowledge-Based Systems* 226 (August 17, 2021): 107120.

[49] Solomon, Rukundo. "Electronic Protests: Hacktivism as a Form of Protest in Uganda." *Computer Law & Security Review* 33, no. 5 (October 1, 2017): 718–28.

[50] Saxena, Rashi, and E. Gayathri. "Cyber Threat Intelligence Challenges: Leveraging Blockchain Intelligence with Possible Solution." *Materials Today: Proceedings*, CMAE'21, 51 (January 1, 2022): 682–89.

[51] Topping, Colin, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid. "Beware Suppliers Bearing Gifts!: Analysing Coverage of Supply Chain Cyber Security in Critical National Infrastructure Sectorial and Cross-Sectorial Frameworks." *Computers & Security* 108 (September 1, 2021): 102324.

[52] Li, Jian, Chaowei Sun, and Qingyu Su. "Analysis of Cascading Failures of Power Cyber-Physical Systems Considering False Data Injection Attacks." *Global Energy Interconnection* 4, no. 2 (April 1, 2021): 204–13.

[53] Marefati, Mohammad, Mehdi Mehrpooya, and Mohammad Behshad Shafii. "Optical and Thermal Analysis of a Parabolic Trough Solar Collector for Production of Thermal Energy in Different Climates in Iran with Comparison between the Conventional Nanofluids." *Journal of Cleaner Production* 175 (February 20, 2018): 294–313.

[54] Patel, Deven C., Mark F. Berry, Prasha Bhandari, Leah M. Backhus, Shehzaib Raees, Winston Trope, Abraham Nash, Natalie S. Lui, Douglas Z. Liou, and Joseph B. Shrager. "Paradoxical Motion on Sniff Test Predicts Greater Improvement Following Diaphragm Plication." *The Annals of Thoracic Surgery* 111, no. 6 (June 1, 2021): 1820–26.

[55] Al Shaer, Danah, Othman Al Musaimi, Beatriz G. de la Torre, and Fernando Albericio. "Hydroxamate Siderophores: Natural Occurrence, Chemical Synthesis, Iron Binding Affinity and Use as Trojan Horses against Pathogens." *European Journal of Medicinal Chemistry* 208 (December 15, 2020): 112791.

[56] Aziz, Amal A., and Zareen Amtul. "Developing Trojan Horses to Induce, Diagnose and Suppress Alzheimer's Pathology." *Pharmacological Research* 149 (November 1, 2019): 104471.

[57] Kharlamova, Nina, Seyedmostafa Hashemi, and Chresten Træholt. "Data-Driven Approaches for Cyber Defense of Battery Energy Storage Systems." *Energy and AI* 5 (September 1, 2021): 100095.

[58] Qiu, Wei, Kaiqi Sun, Wenxuan Yao, Shutang You, He Yin, Xiaoyang Ma, and Yilu Liu. "Time-Frequency Based Cyber

Security Defense of Wide-Area Control System for Fast Frequency Reserve." *International Journal of Electrical Power & Energy Systems* 132 (November 1, 2021): 107151.

[59] Lee, Chanyoung, Young Ho Chae, and Poong Hyun Seong. "Development of a Method for Estimating Security State: Supporting Integrated Response to Cyber-Attacks in NPPs." *Annals of Nuclear Energy* 158 (August 1, 2021): 108287.

[60] "Bayesian Stackelberg Games for Cyber-Security Decision Support - ScienceDirect." Accessed March 27, 2022.

[61] Kim, Yong Sik, Moon Kyoung Choi, Sang Min Han, Chanyoung Lee, and Poong Hyun Seong. "Development of a Method for Quantifying Relative Importance of NPP Cyber Attack Probability Variables Based on Factor Analysis and AHP." *Annals of Nuclear Energy* 149 (December 15, 2020): 107790.

[62] Tosun, Onur Kemal. "Cyber-Attacks and Stock Market Activity." *International Review of Financial Analysis* 76 (July 1, 2021): 101795.

[63] Rodríguez-deArriba, María-Luisa, AnnaLaura Nocentini, Ersilia Menesini, and Virginia Sánchez-Jiménez. "Dimensions and Measures of Cyber Dating Violence in Adolescents: A Systematic Review." *Aggression and Violent Behavior* 58 (May 1, 2021): 101613.

[64] Zhang, Jie. "Distributed Network Security Framework of Energy Internet Based on Internet of Things." *Sustainable Energy Technologies and Assessments* 44 (April 1, 2021): 101051.

[65] Alkatheiri, Mohammed Saeed, Sajjad Hussain Chauhdary, and Mohammed A. Alqarni. "Seamless Security Apprise Method for Improving the Reliability of Sustainable Energy-Based Smart Home Applications." *Sustainable Energy Technologies and Assessments* 45 (June 1, 2021): 101219.

[66] Ogbanufe, Obi. "Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity." *Computers & Security* 108 (September 1, 2021): 102340.

[67] Krishnasamy, Vidhyanandhini, and Saravanarajan Venkatachalam. "An Efficient Data Flow Material Model Based Cloud Authentication Data Security and Reduce a Cloud Storage Cost Using Index-Level Boundary Pattern Convergent Encryption Algorithm." *Materials Today: Proceedings*, May 26, 2021.

[68] Palmieri, Michael, Neil Shortland, and Presley McGarry. "Personality and Online Deviance: The Role of Reinforcement Sensitivity Theory in Cybercrime." *Computers in Human Behavior* 120 (July 1, 2021): 106745.

[69] Nguyen, Dr. Chat Le, and Dr. Wilfred Golman. "Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action.'" *Computer Law & Security Review* 40 (April 1,

2021): 105521.

[70] Alzubaidi, Abdulaziz. "Cybercrime Awareness among Saudi Nationals: Dataset." *Data in Brief* 36 (June 1, 2021): 106965.

[71] Chandra, Akhilesh, and Melissa J. Snowe. "A Taxonomy of Cybercrime: Theory and Design." *International Journal of Accounting Information Systems*, 2019 UW CISA Symposium, 38 (September 1, 2020): 100467.

[72] Huang, Jiahao, Daniel W. C. Ho, Fangfei Li, Wen Yang, and Yang Tang. "Secure Remote State Estimation against Linear Man-in-the-Middle Attacks Using Watermarking." *Automatica* 121 (November 1, 2020): 109182.

[73] Katrakazas, Christos, Athanasios Theofilatos, George Papastefanatos, Jérôme Härri, and Constantinos Antoniou. "Chapter Three - Cyber Security and Its Impact on CAV Safety: Overview, Policy Needs and Challenges." In *Advances in Transport Policy and Planning*, edited by Dimitris Milakis, Nikolas Thomopoulos, and Bert van Wee, 5:73–94. Policy Implications of Autonomous Vehicles. Academic Press, 2020.

[74] Tam, Tracy, Asha Rao, and Joanne Hall. "The Good, the Bad and the Missing: A Narrative Review of Cyber-Security Implications for Australian Small Businesses." *Computers & Security* 109 (October 1, 2021): 102385.

[75] Cheng, Shen, Gaiju Zhao, Ming Gao, Yuetao Shi, Mingming Huang, and Mohammad Marefati. "A New Hybrid Solar Photovoltaic/ Phosphoric Acid Fuel Cell and Energy Storage System; Energy and Exergy Performance." *International Journal of Hydrogen Energy* 46, no. 11 (February 11, 2021): 8048–66.

[76] Alghamdi, Mohammed I. "Determining the Impact of Cyber Security Awareness on Employee Behaviour: A Case of Saudi Arabia." *Materials Today: Proceedings*, April 29, 2021.

[77] Sakhnini, Jacob, Hadis Karimipour, Ali Dehghantanha, and Reza M. Parizi. "Physical Layer Attack Identification and Localization in Cyber–Physical Grid: An Ensemble Deep Learning Based Approach." *Physical Communication* 47 (August 1, 2021): 101394.

[78] Baig, Zubair A., Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, et al. "Future Challenges for Smart Cities: Cyber-Security and Digital Forensics." *Digital Investigation* 22 (September 1, 2017): 3–13.

[79] Arend, Isabel, Asaf Shabtai, Tali Idan, Ruty Keinan, and Yoella Bereby-Meyer. "Passive- and Not Active-Risk Tendencies Predict Cyber Security Behavior." *Computers & Security* 97 (October 1, 2020): 101964.

Erej *et al.LGU (IJECI)* 2022

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

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 6 issue 2 Year 2022

# Data Carving - The Art of Retrieving Deleted Data as Evidence

**Fatima Fatima and Erej Azeem**
Government College University, Lahore
erejazeem00@gmail.com,

**Abstract:**
This paper proposes an approach to extract the hidden information as sensitive data can be hidden by the criminal in free space or slack space. But their might be cases when there exists no file system meta data information for file recovery. For this purpose Data Carving techniques are used by forensic examiners. If a file is carved in a forensically sound manner, it is then acceptable in the court of law. Many automated tools exist to carve data out of a hard drive. In this paper we looked on how to carve data in an old fashioned way followed by carving data using tools.

**Keywords:** Digital Forensics, Hard disk forensics, Data Carving, File system, Autopsy, Forensic Explorer, Unallocated space, file signature, manual extraction

## 1. Introduction

Today we regard ourselves as in a computerized world, where most data is made, caught, communicated, put away, and handled in computerized structure. From house to the industry, computers have become a everyday thing and there has been a massive increase in the crimes associated with it. This is where Digital Forensics come in. The focus of the forensic science discipline known as "digital forensics" is the use of digital information produced, saved, and conveyed by computers as a source of evidence in investigations and legal procedures. Digital forensic analysis makes it possible to recognize the type of crime committed and the culprit behind the crime. The main source of evidence against such crimes is the computer hard disk [1]. Investigator can perform forensic investigation of the file system on the hard disk to gather evidence against the criminal. Suspect might hide some sensitive information in the free space or the slack space of the file system therefore there is a need of forensic investigation of these spaces to retrieve the sensitive information [2]. Data storage on hard disk drive are organized by the file system, it is responsible for allocating free space to the files and to keep track of those files. To extract data

from unallocated space examiners use the technique of Data carving. Even though it is advantageous to comprehend the procedure and have the ability to carry it out manually if necessary, there are a lot of utilities that can carry out this activities for us.

There are different situations in which we carry out the process of Data carving. Such as, if you open a file, it can appear to be one thing when in reality it's two things since the contents may have been stuffed into another file. You might have data that is simply stored outside the reach of several widely used operating system functions in situations where you have forked data, such as an alternate data stream or a resource fork [3]. We therefore carry out data carving. However, in order to extract data from a hard drive, we must first understand what we are looking for and how far to search. Since we are dependent on byte patterns on the drive, adopting this data carving strategy has several drawbacks. It cannot be guaranteed that byte patterns like "ff d9" will only appear in the files we are looking for. The most frequent instance of carving in an actual investigation is an attempt to recover deleted data for which the associated metadata is either missing or no longer linked.

## 2. Data Carving

A wise forensic examiner once said "when all else fails, we carve". Data carving, also known as File carving is a forensic procedure that is used for reconstructing files in unallocated space. It is also an effective skill for the recovery of deleted data from unallocated memory space by locating the file signatures or the magic numbers.

There are several issues that an examiner may face during the process of Data Carving. Such as, the majority of tools would be able to locate the header, but it is possible that the footer would not be in the same or subsequent cluster. Thus, the carved file may be incomplete and may not be viewable. Data carving process can also result in many false hits, therefore, Footer analysis may reduce this problem. For several reasons file system information may not be available at some point, digital media could have been formatted to destroy the file system or a specific file might have been removed or deleted such that the file system indexes stop referring to the file content or maybe a file might be hidden in slack space or unallocated clusters [4]. A file recovery process or the process of recovering deleted data by locating the file signatures is basically known as File carving or Data carving. Raw bytes of the disk are scanned for the file carving process and then reassembled by examining the file signature.

File Signatures are also termed as **Magic numbers** which is a constant used for identifying the file format and distinguishing between the file formats, this means two different file types cannot have same File signatures. For example a JPEG file begins with "**0xFFD8**" and ends with "**0xFFD9**". These constants are called File signatures or Magic numbers. File signatures can be altered which can result in fake file type identification.

Depending upon the situation, various tools for Data carving can be used by the examiner. However, it is required that the examiner clearly understands the features of the tool and has a clear concept of carving a file. Currently, many Data carving commercial tools exists.

Namely, Encase, Win-hex, Access-data FTK, foremost, scalpel and many more.

If we talk about Windows Operating System, space is allocated on the hard disk drive as adjoining sectors in the form of group which are also known as clusters or allocation units. Whenever a new file is created, available space is found by the system and that space is allocated to that file. Unallocated space can be defined as the space that is not allocated within the file system to the active files [5]. This space is also sometimes called free space and on a hard drive it is a logical space on which Windows operating system can write to. It is basically opposing of allocated space, where files are already written by the operating system.

Data might by hidden by the criminal in slack space. The remaining storage on a computer's hard disk drive is the Slack space and it when an operating system allocates a space to the file and all of that space is not needed by the file. In other words, The portion after the end of a file but before the end of a cluster or block is usually referred to as slack space. In computer forensics, the analysis of Slack space is a very important aspect. In forensic investigations, it can be an important form of evidence. For example, if an entire hard disk cluster is filled by a file and the user deletes that file, and then a new file is saved by the user that does not entirely fill the hard disk cluster then the leftover space would not be necessarily be empty, it may contain data from the deleted file. Forensic examiners can extract that information using computer forensics tools.

In the following figure 1, one cluster is shown that is of 4096 bytes containing 8 sectors of 512 bytes each represented as S1, S2, S3 .. S8 respectively.

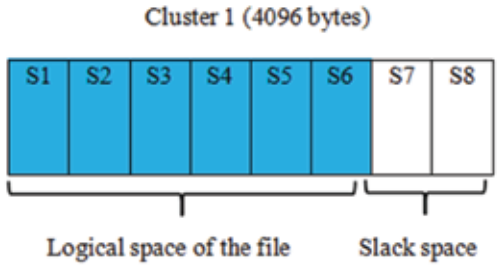



**Figure 1:** Slack space explanation

To destroy the evidence, file deletion is one of the effortless way. Whether by using "DELETE" or "SHIFT + DELETE" button. Whenever the file is being deleted, the contents of the file are not wiped. Windows use the concept of pointers to track where the files exist on the hard disk drive. Every file and folder has a pointer. When a file is deleted, the pointer is removed and the sectors that contain the data of the file are marked as "available". The file content is recoverable until and unless those sectors are overwritten. If a person does not wants his/her data to be recovered, they can use tools that wipes hard disk drives free space.

## 2.1 Difference between File Recovery and File Carving

One might be confused between the term file recovery and data carving. By using some forensics tool we can recover the deleted file until and unless it is not overwritten by any other file [6]. File system information is used for the purpose of file recovery and many files can be recovered by using the file system information. Whereas, file carving or data carving works on raw data. File system information is

not used during the process of file carving. In Data carving, a file is recovered on the basis of content and the structure of the file without the involvement of any matching file system meta data. If there is a case like corrupt directory entries or the missing directory entries, file carving technique is effectively used. All we are looking at when it comes to data carving is a collection of bytes on a disc. It basically comes down to finding the drive's header bytes and then just extracting data from succeeding bytes.

### 2.2 Importance of Data Carving

Data carving is a crucial aspect in Digital forensics because it is a considerate technique in detecting a deleted file. A file can be hidden or concealed anywhere in areas like lost clusters, slack space, unallocated clusters of the hard disk drive. Forensic investigators may be sometimes in a situation where they are required to recover data. But why Data Carving? When the data is there, but can't be correctly interpreted due to absent or damaged meta-data. For examples: File system corruption, Device formatting, Unknown proprietary formats, Files removed or deleted (unintentionally or intentionally).

Traditional data recovery techniques are based on the file system information and the metadata information is used to recover deleted files. However their might be some cases where there is no metadata information available and for such cases advanced forensic techniques are used such as Data carving. Files can be recovered through data carving as long as they are not overwritten.

A file system can store information in a variety of methods, and that information and data may persist long after the user thinks it has gone. This is crucial information for forensics experts because a suspect can try to conceal evidence, so you'll need to know not just where it might still be but also how to get to it. Data carving skills are crucial for this reason.

## 3. Acceptable Evidence

Any document, physical item or testimony that can be used for proving a fact under the rules of evidence in a court of law. The admissibility of the evidence depends on various components. Those evidence that does not fall under the law of evidence are entitled as "inadmissible". During file carving there is a complication that has to do with fragmented files. By fragmented files we mean a file that is stored on the disk at two or more different physical locations. And some techniques cannot reconstruct these types of files. Carving is done on the basis of file signatures and unfortunately not all file types have a standard footer signature and therefore locating the end of file is difficult. But if a file is carved in a forensically sound manner, it is then acceptable in the court of law [7]. Forensic soundness provides assurance that during the investigation the evidence was not destroyed or corrupted.

## 4. Manual Data Carving

Many automated tools exist to carve data out of a hard drive. In this section we will see how an investigator or examiner can perform manual Data carving by locating the file signatures. Basically, We will look on how to carve data in an old fashioned way. To extract data we will use UNIX utilities [8]. First we created an image of a 4GB USB rather than using a raw

partition using the command;

**sudo dd if=/dev/sdb1 of=image.dd**

**Figure 2:** Creating Forensic image

Now we will find the headers of PNG file using the command;

**grep -oba IHDR image.dd**

And after running this command we get number of headers in the image file. “IHDR” is the PNG file header.

**Figure 3:** Checking Headers of PNG file

And similarly we can find the footers of PNG file using command;

**grep -oba IEND image.dd**

The ”IEND” chunk must appear LAST. It marks the end of the PNG data stream.

Figure 4 shows how we find out our starting sector, ending sector and block size.

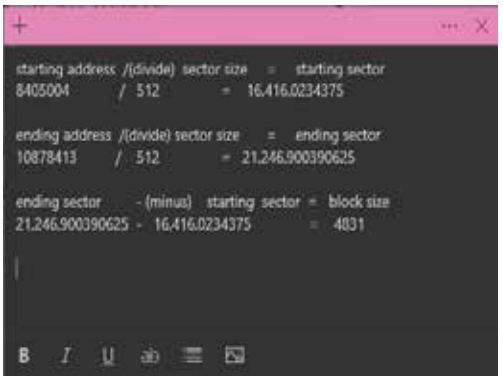



**Figure 4: Starting/ending sector, block size**

Now we have all the information about our PNG file. let’s carve our PNG file from image.dd file using command;

**dd if=image.dd of=img.png bs=512 skip=16416 count=4831 command.**

**Figure 5: Carving file**

We successfully extracted the PNG file from image.dd File named img.png.

**Figure 6: File extracted**

## 5. Data Carving using HEX Editor

File carving is a technique for getting erased or reassembled computer files. It entails looking for a file within a data stream. This step is important in digital forensics because the forensics expert must examine all of the file system files and check for any deleted or formatted files that need to be further investigated. We can use any HEX editor such as WinHex and HxD to perform the process of Data Carving. Download the image file from here;

http://sceweb.sce.uhcl.edu/abeyseker-a/ITEC4381/images/Mantooth.E01

Steps to perform Data Carving using HEX Editor;

i. Our objective in manual data carving is to locate a JPG file. Now in the HEX we will find header of a JPG file by simply right clicking or "CTRL + F" and the header for a JPG file is "FF D8".


**Figure 7:** Location JPG header

ii. We got the starting point and on the left side we can see the digital offset "90640896" in figure 3.

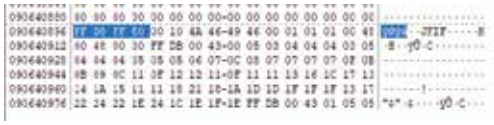


**Figure 8:** Header of a JPG file

iii. Now the next step is to find the footer for the JPG file. The footer for the JPG file is "FF D9" and we will follow the same procedure we followed for locating the file header that is by simply right clicking or "CTRL + F".

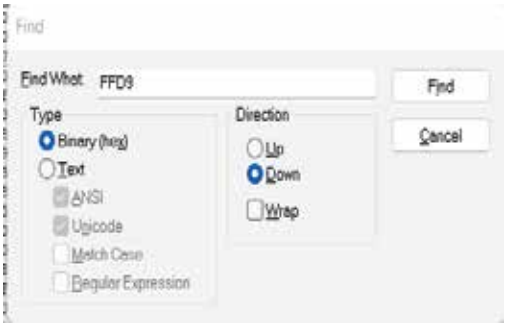



**Figure 9:** Locating the footer of JPG file

iv. We have successfully located the footer of the JPG file, that is the Ending of the file. As it can be seen in figure 5, "FF D9" has been highlighted with its digital offset 90659280". In other words we have got the starting and the ending point of the JPG file.

**Figure 10:** Footer of the JPG file

v. If we notice figure 3 and figure 5, we have digital offset 90640896 in figure 3 and digital offset 90659280 in figure 5. We will subtract 90640896 from 90659280 and we get 18400 which is the selection size of the JPG file.

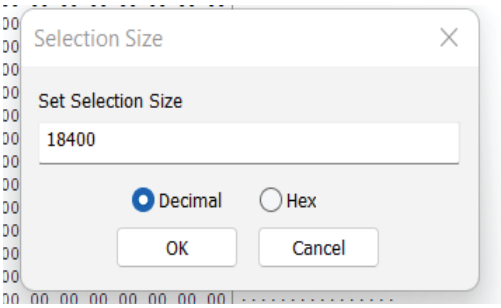



**Figure 11:** Defining the selection size of the JPG file

vi. We then save the file with JPG extension. And file is therefore recovered. Viewing the JPG file, we can see this is one of the JPG file that was also carved using Forensic Explorer and Autopsy software.

**Figure 12:** JPG File recovered by manual Data carving process.

### 5.1 Data Carving using other Tools

Tools like Forensic Explorer and Autopsy can be used for the purpose of Data Carving. Forensic Explorer is a tool that can be used by both novice and experienced investigators. This tool provides easy to use graphical user interface (GUI) followed by keyword search, data recovery, script technology, sort and filter. Large volume of data is quickly processed, complex investigative tasks are efficiently automated, detailed reports are produced and productivity is thereby increased. On the other hand, A digital forensic platform, Autopsy is used by corporate examiners and investigators, law enforcement agencies and military for digital forensic investigations for data carving.

Carving support offered by Forensic Explorer is for mare that 300 file types. It supports Cluster based file carving, Sector based file carving and also the Byte based file carving. In FAT or NTFS, which are the cluster based file system, a new file must start in a new cluster. The file signature then appears near the file boundary so the file signatures are therefore searched near the file boundaries and the carving speed is then achieved. Their might be some situations in which performing lower level search for sector aligned file signatures may be advantageous, additional files can be recovered. Time needed to complete search is increased when carving in sector mode. And in some situations, carving data on byte by byte level may be of great importance [9]. A byte based data carve is used when we are searching for a file that exists within a file. For example, within a backup file. A **Robust Pascal Scripting** engine is offered by Forensic Explorer where writing of data carving scripts is possible.

Whereas, Autopsy comes with a module named **Photo Rec Carver** that is used for Data carving and carves files from unallocated space [10]. The module works on the same principle of locating the File signatures i.e. headers and footers. For using this module the examiner just needs to select the checkbox in the ingest module settings and then the Photo

Rec Carver is enabled. Under the tree of Data Sources, results of carving are shown with the heading "$CarvedFiles".

### 5.1.1 Comparison between Carved files using Forensic Explorer and Autopsy

Following table shows a comparison of carved files between Forensic Explorer and Autopsy using the same Forensic image "mantooth".

| | Forensic Explorer | Autopsy |
|---|---|---|
| **GIF** | 0 | 1 |
| **REG** | 0 | 2 |
| **JPG** | 5 | 5 |
| **DOC** | 6 | 6 |
| **TXT** | 368 | 0 |
| **DAT** | 2 | 0 |
| **NTFS** | 1 | 0 |
| **PNG** | 0 | 1 |

It can be seen that 1 GIF, 2 REG, 5 JPG, 6 DOC and 1 PNG file is carved by Autopsy. Whereas, 5 JPG, 6 DOC, 365 TXT, 2 DAT and 1 NTFS files are carved by Forensic Explorer. A plus point for Forensic Explorer is that it provides a Disk view and a category graph which provides convenience for the examiner to categorize the file types.

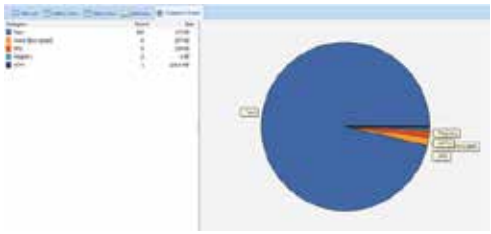


**Figure 8:** Forensic Explorer Category graph

## 6. Conclusion

Digital forensics, field of file recovery is still growing and has made progress in the recovery of transient data. In conclusion, this paper covered the basics of Data carving in which we described data carving along with other important concepts of slack space, unallocated space and Magic numbers. We performed file carving using the tools and HEX editor and on the other hand we also touched the area of manual data carving using UNIX utility. Furthermore advancement of tools for data carving process will have a greater impact. However, data carving remains a beneficial technique for the recovery of files and potential evidence without using any file system meta data information during digital investigations. There is a lot of research yet to be done in the area of data recovery. File carving technique is greatly used by the forensic experts and the examiners to squeeze every bit of data out of the media. However, carving is impossible if a new file has already been overwritten in the unallocated area where the old file was placed.

## 7. References

[1] Povar, Digambar, and V. K. Bhadran. "Forensic data carving." International Conference on Digital Forensics and Cyber Crime. Springer, Berlin, Heidelberg, 2010.

[2] Meshram, Bandu B., and Dinesh N. Patil. "Digital Forensic Analysis of Hard Disk for Evidence Collection." International Journal of Cyber-Security and Digital Forensics, vol. 7, no. 2, Apr. 2018, pp. 100+. Gale Academic OneFile,

link.gale.com/apps/-doc/A568570241/AON-E?u=anon~9c67264d&sid=-googleScholar&xid=28bb2ba3. Accessed 23 Aug. 2022.

[3] Alherbawi, Nadeem, Zarina Shukur, and Rossilawati Sulaiman. "Systematic literature review on data carving in digital forensic." Procedia technology 11 (2013): 86-92.

[4] Povar, Digambar, and V. K. Bhadran. "Forensic data carving." International Conference on Digital Forensics and Cyber Crime. Springer, Berlin, Heidelberg, 2010.

[5] Povar, Digambar, and V. K. Bhadran. "Forensic data carving." International Conference on Digital Forensics and Cyber Crime. Springer, Berlin, Heidelberg, 2010.

[6] A. Pal and N. Memon, The Evolution of File Carving, IEEE Signal Processing Magazine, no.March, pp. 59-71, 2009.

[7] Meyers, Matthew, and Marc Rogers. "Computer forensics: The need for standardization and certification." International Journal of Digital Evidence 3.2 (2004): 1-11.

[8] Cantrell, Gary D., and Joan Runs Through. "Teaching Data Carving Using The Real World Problem of Text Message Extraction From Unstructured Mobile Device Data Dumps." Journal of Digital Forensics, Security and Law 14.4 (2020): 4.

[9] Beek, Christiaan. 2011. Introduction to File carving. McAfee

[10] Pahade, Raj Kumar, Bhupendra Singh, and Upasna Singh. "A survey on multimedia file carving." International Journal of Computer Science & Engineering Survey 6.6 (2015).

Syeda Mona *et al.LGU (IJECI) 2022*

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

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 6 issue 2 Year 2022

# New Perspective of Calcium Oxide Nanoparticles in Forensic Science

**Dr. Syeda Mona Hassan[1], Dr. Aftab Ahmad Malik[2] and Hafiza Hadia Shehzad[3]**

[1] Department of Chemistry, University of Agriculture, Faisalabad

[2] Faculty of Computer Sciences and Engineering, Ghulam Ishaq Khan Institute of Science and Engineering, KPK

[3] Department of Chemistry, University of Education, Lahore.

## Abstract:

Nano-technologies have wide applications in the field of forensic science. Nanotechnology is an important and powerful tool in most the areas including medicine, imaging, and forensic sciences. It has potential to make significant positive contribution in forensic science in crime detection. The present article focuses on the applications of CaO nanoparticles in developing and detecting the latent fingerprints. Fingerprint is considered noteworthy evidence in any crime scene, and nano-based techniques. An attempt was made to elucidate how nanotechnologies could be crucial in addressing current forensic investigation issues such as explosive detection, toxicological analysis, finger print analysis, forensic DNA analysis, detection of explosive residue, forensic nano trackers and drug facilitated crime.

**Keywords:** Nanotechnology, Forensic investigation, Nano trackers, DNA analysis, explosive detection

## 1. Introduction

Although scientists and technologists are still being inspired by nanotechnology to investigate novel materials and human benefits (Patel *et al.*, 2008).

Nanotechnology is the study of the atomic or molecular processing of materials with at least one dimension in the 1–100nm range that result from controlled synthesis. Since the very first forms of life on earth, like plants and animals, were molecularly altered to create their structures, this fascinating technology is not new to nature. One can find inspiration to develop nanoscale materials by engaging in extensive observation and improving awareness of nature's fundamental design principles. This interesting field of study is made possible by the examination of nanoscale technology and how they interact with nature (Sheeparamatti, Sheeparamatti, & Kadadevaramath, 2007).

These NPs are well known for their intrinsic antimicrobial activity and have potential applications in food, climate and healthcare. CaO NPs stand out among them for their superior

antibacterial power and capacity to inactivate microbial endotoxin. In photodynamic therapy, they may be utilized as a potential medication delivery system due to CaO NPs specific structural and photothermal therapy (PTT), optical properties (PDT) and synaptic distribution of chemotherapeutic agents.

Conformational changes in albumin association with NPs play a critical role in diverse biomedical applications. Thanks to its broad variety of physiological functions, BSA is a good model for studying protein conformational changes, a suitable protein for intrinsic fluorescence measurements, well characterized structure and property, and readily undergoing conformational changes, target the desired organ. When NPs enter a biological fluid there will be changes in conformation and biological activity of protein as well as modification in the properties of NPs (Gross *et al.*, 2012).

The term "nanotechnology" soon captured the imagination and curiosity of the general public as well as of various media (TV networks, the internet, etc.). Nanoparticles typically range in size from 1 to 100 nanometers. Metallic nanoparticles have various physical and chemical features from bulk metals, including as lower melting temperatures, higher special surface areas, unique optical qualities, mechanical prowess, and unique magnetization, which could be advantageous in a variety of industrial applications (Roco, 2011).

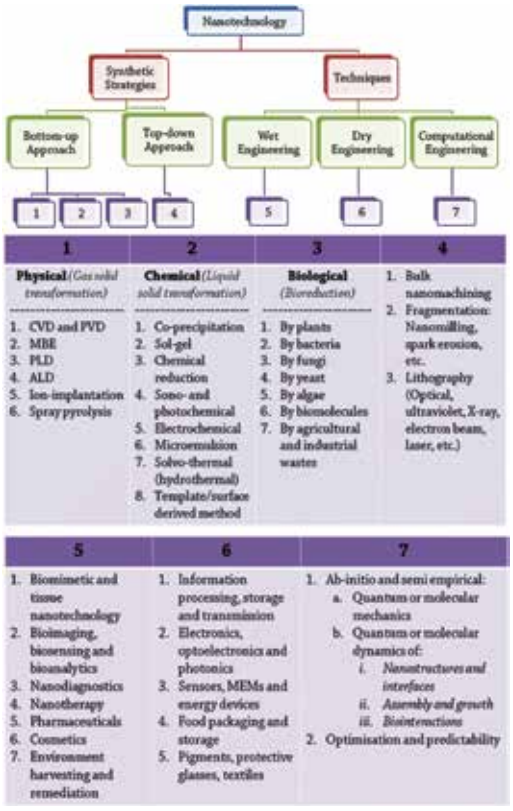




Table 2.1: The use of Nanotechnology techniques in manufacture

Nanoparticles typically range in size from 1 to 100nanometers. The description of nanoparticles and nonmaterial's by different organizations is outlined in this respect. In special interest, one of the fundamental attractions and a hallmark of nanoparticles is the optical property. A 20nm gold nanoparticles, for example, has a distinctive red wine hue. The size of the nanoparticles utilized in the field of biotechnology typically ranges between 10 and 500nm. Due to their small size, these particles can interact with biomolecules inside and on the surfaces of cells in a number of ways that can be interpreted and assigned to various biochemical and physiochemical properties of these cells (Mody *et al.*, 2009).

The systems for nanoparticles must be stable, biocompatible, and selectively directed to particular places in the body following systematic delivery if they are to be used to their full potential. To recognize the targeted cells in an administration, more precise targeting systems are created. If in at least one of their lengths, nanoparticles are smaller than 100nm. In general, however, nanoparticles are materials which have nanoscale dimensions of at least two dimensions, including particles as well as fibrous materials and tubes, but excluding nanoscale materials of only one dimension, such as coatings, films and multilayer's (Holister *et al.*, 2003).

There are many types of particles under this umbrella word, which only have the resemblance of their small size. The word of "nanoparticles" is commonly used as a collective term in this study as well as in the everyday language. However, it is important to remember that it (Biswas *et al.*, 2005).

In various fields of science and technology, nanotechnology has broad applications and recent research focuses on NPs related materials and their applications. Much of the size of biological molecules is close to that NPs, because it has uses in both in vitro and in vivo biochemical studies. NPs have possible applications in drug distribution, "a wonder of nano medicine" cancer therapeutics, in antibacterial vaccinations to manage bacterial infections and to target bacteria as an alternative to antibiotics. Inorganic nano metal oxide NPs (MgO, CaO, CuO, ZnO, $TiO_2$) have distinct features and are safe, stable and possess multifunctional properties (Ranghar *et al.*, 2014). These NPs are well known for their intrinsic antimicrobial activity and have potential nutritional, environmental and health care applications. Among these, CaO NPs have outstanding antimicrobial potential and ability to inactivate microbial endotoxin.

Due to the unique structural and optical characteristics of CaO NPs, they have the potential to be employed as a drug delivery agent in photodynamic therapy (PDT), photo thermal therapy (PTT), and synaptic delivery of chemotherapeutic drugs. CaO nanoparticles are non-toxic to both people and animals. Conformational changes in albumin association with NPs play a critical role in diverse biomedical applications. Thanks to its broad variety of physiological functions, BSA is a good model for studying protein conformational changes, an excellent protein for intrinsic fluorescence measurements, well characterized structure and property, and easily undergoes conformational changes.

Many therapeutic nano systems, targeting the target organ, are configured for intravenous systematic administration. Changes in protein conformation and biological behavior and alternation of the properties of NPs can occur as NPs join a biological fluid (Gross *et al.*, 2012).

## 2. Nanoparticles

A particle with a size of at least one of the three possible dimensions between 1nm and 100nm is referred to as a "nanoparticle." In fundamental aspects, the physical, chemical, and biological characteristics of nanoparticles differ from those of all individual atoms or molecules and the associated bulk materials in this size range. Metals, non-oxide metal ions, metal oxides, ceramics, polymers, organic materials, carbon, and biomolecules the most prevalent chemical

components used to make nanoparticles (Roco *et al.*, 2011).

Back in 2000, the United States initiated the almost all of the United States' states rapidly launched their own nanotechnology efforts after the National Nanotechnology Initiative(NNI) (2001). National Science Foundation departments ultimately sponsored approximately 20 research Centre (NSF), an organization that is directly accountable to the president of the United States to bring out the NNI (Moreno-Olivas *et al.*, 2014).

Recently, microbial bioprocessing has been investigated as a desirable an option to creating nanoparticles chemically and physically. Nanotechnology and microbial biotechnology are combined during the microbial synthesis of NPs. Exploration of bacteria, archaebacterial, fungus, yeast, moulds, microalgae, and viruses is being done in order to create bioactive nanostructures that have many industrial benefits (Hulkoti *et al.*, 2014).

Most of the time, microbial biosynthesis and bioprocessing results in cost-efficient, environmentally beneficial, and sustainable NPs. However, the biogenesis process takes a long time, and it is challenging to regulate the NPs' size, shape, and dispersion. To get beyond these restrictions, a number of ways have been developed, including proper strain selection, the creation of genetically modified microbes, the development of technologies for extracting and cultivating microorganisms, as well as combination techniques such photo-biological procedures (Mohammadian *et al.*, 2016).

Nanoparticles come in a variety of distinct morphologies, including spheres, tubes, platelets, and cylinders, among others. In general, nanoparticles have their surfaces modified to match the requirements of the particular applications they will be used in. the vast chemical diversity of nanoparticles that results from it. The particle's morphologies, state of particle dispersion, medium in which it is present, and, most importantly, the different potential surface alterations the nanoparticles can be exposed to, are necessary to make this an essential active area of research today (Cunill *et al.*, 2019).

## 3. Classification of Nanoparticles

The organic, inorganic, and carbon-based nanoparticles are the three main categories for the nanoparticles.

### Organic Nanoparticles

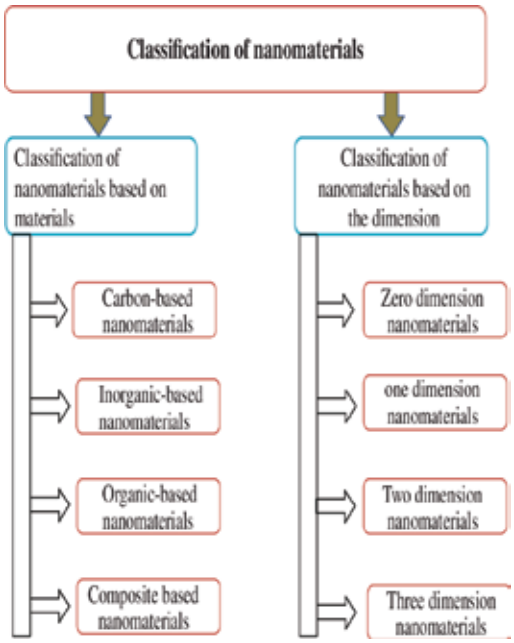
Organic nanoparticles or polymers include ferritin, liposomes, dendrimers, and micelles. Some of these nanoparticles, such as micelles and liposomes, are biodegradable and non-toxic, own hollow cores that give them the name "nanocapsules" and make them sensitive to electromagnetic and thermal radiation like heat and light. They are the perfect option for drug administration because of their distinctive qualities. In addition to their normal characteristics like size, composition, surface form, etc., the drug carrying capacity, stability, and delivery systems whether entrapped drug or adsorbed drug system determine their range of applications and efficiency. The biomedical sector uses organic nanoparticles most frequently for drug delivery systems because they are efficient and may be injected into specific physiological locations, a procedure known as targeted medicine administration.

### Inorganic nanoparticles

Nanoscale metal particles Inorganic nanoparticles are those that are not made of carbon. Metallic nanoparticles are often classified as those made of metal or metal oxide.

## 4. Carbon based

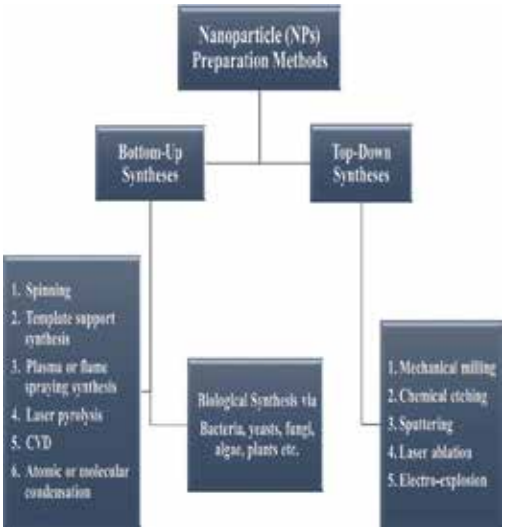
All-carbon nanoparticles are known as carbon-based nanoparticles. Fullerenes, graphene, carbon nanotubes (CNT), carbon nanofibers, carbon black, and on occasion activated carbon are used to represent them (Ealia & Saravanakumar, 2017).




## 5. Green Synthesis of Nanoparticles

There are many methods for the preparation of nanoparticles, but most common method we used are the

1. Top down approach
2. Bottom up approach (Iravani, 2011).




## 6. CaO Nanoparticles

Calcium oxide nanoparticles are used in photo thermal and photodynamic therapy and synaptic delivery as potential drug delivery agents. CaO NPs are also used in different fields with potential biomedical applications, such as electronics, environmental remediation, sensors and catalysis (Kumar *et al.*, 2019).

Calcium oxide (CaO) is the most significant substance that has been widely utilised in a variety of fields, including catalysis, cosmetics, and ceramics to control microorganisms, it is also used as an inorganic antimicrobial substance. Depending on its chemical makeup, CaO can be found in the periodic table's alkaline earth (Marquis *et al.*, 2016).

However, given the great richness of tropical plants group found in Indonesia, using tropical biomass or its extract for CaO biosynthesis would be a worthy scientific challenge due to the more efficient and environmentally friendly method of CaO biosynthesis. The ability of a metabolite chemical found in plant materials to

act as a biological reducer for metal production is well established (Akhtar *et al.*, 2013). Where flavonoids compounds were found to be one of the most useful classes of plant tissue secondary metabolites added as a reducing a metal ion agent.

Depending on the type of plant, the majority of flavonoids compounds naturally contain natural colours in various shades, such as red, pink, and purple. Calcium oxide is the most significant substance that has been widely utilised in a variety of fields, including catalysis, cosmetics, and ceramics (CaO). It is also employed as an inorganic antibacterial agent to inhibit germs. Depending on its chemical makeup, CaO belongs in the periodic table's alkaline earth group. However, given the great richness of tropical plants found in Indonesia, using tropical biomass or its extracts for CaO biosynthesis would be a worthy scientific challenge due to the more efficient and environmentally friendly method of CaO biosynthesis. It is generally recognised that chemicals found in plant materials, such as biomass, can act as biological compounds on the production of metals (Mustafa *et al.*, 2013).

Where flavonoids compounds were found to be one of the most useful classes of plant tissue secondary metabolites added as a reducing agent for ions of metal. Depending on the shape of the plant, many flavonoids naturally create natural pigments in a variety of hues, such as red, pink, and yellow. The previous ten years, researchers have concentrated immensely on nanotechnology and intensely on nanotechnology efforts to investigate the electrical, optical and magnetic properties of nonmaterial. A number of nanoparticles-based therapeutics have increased effectiveness and decreased the toxicity of drugs, biological obstacles and selective drug delivery agents. These peculiarities can be modulated for large nano-biomedical applications (Choi & Han, 2018).

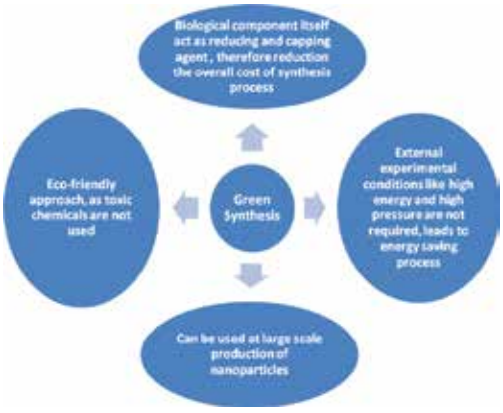
## 7. Green Chemistry

The field of "green chemistry," which was established two decades ago, represents the key efforts to address such challenges from the most fundamental level by re-examining, redesigning, and recreating the scientific tools used in the production, transformation, and use of chemical products in order to increase efficiency while reducing waste and harm. The objectives of this issue on green chemistry, which includes some of the leading professionals in the field, are to assess our needs in the area, reflect on the advancements made, and celebrate successes. This selection merely scratches the surface of the countless intriguing developments in the area (Iqbal *et al.*, 2020).

All areas of chemistry are included in "green chemistry," however there is a particular emphasis on chemical compound synthesis and chemical engineering techniques used in industrial settings using natural materials. On the other hand, laboratory investigations are also impacted by the key principles of green chemistry, creating a safer environment. According to sustainable chemistry, or "green chemistry," the use and production of hazardous compounds are reduced during reaction and synthesis. Green chemistry also involves processes for creating renewable materials. The following are the primary objectives of green chemistry, the utilization of renewable materials and energy sources, as well as the design of reactions with the highest efficiency. Using green chemistry, new nonmaterial can

be created that have positive effects on the economy, society, health, and environment (Ramesh *et al.*, 2012).

Synthesis of many green nanoscale drug delivery systems this will be stressed first. The vast majority of examples for the use of green chemistry in nanoscale drug delivery systems rely on gold nanoparticles (AuNPs), polymer nanoparticles, and biological drug delivery systems based on proteins and lipids. Following each section is a quick summary of the green manufacturing companies that are currently being developed. Last but not least, a focus will be given on the future paths that the field of green nano-chemistry needs to take in order to eventually apply green chemistry in nanomedicine on a large scale to safely and successfully treat a variety of disorders (Bernardini *et al.*, 2015).




## 8. Parameters Effecting Green Synthesis of Metal Nanoparticles

Different parameters, such as reaction time, reactant concentrations, pH, and temperature, can be used to alter the morphological properties of nanoparticles (Table 1.1). Such factors are important for knowing the effect of environmental conditions on nanoparticles synthesis because they plays an important role in optimizing the metallic nanoparticle's synthesis through biological means (D. Zhang *et al.*, 2020).

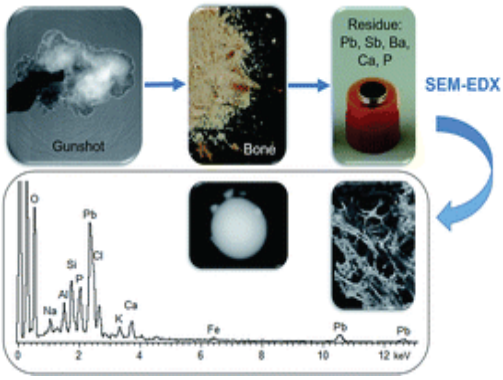
| S. No. | Factors | Effect on green synthesis ofmetal NPs | References |
|---|---|---|---|
| 1 | pH | Shape and size of NPs | (Dubey *et al.*, 2010) |
| 2 | Reactant concentration | Shape of NPs | (Chandran *et al.*, 2006) |
| 3 | Reaction time | Shape and size of NPs | (Prathna *et al.*, 2011) |
| 4 | Reaction temperature | Yeild, shape stability and size of the NPs | (Yong Song *et al.*, 2009) |

## 9. Application of Nanotechnology in Forensic Science

### Forensic GSR Analysis

CaO nanoparticles of forensic science relies heavily on gunshot residue (GSR) to determine specific elements of crime. CaO nanoparticles is used of a gun resulted in a suicide or a murder is the major goal of GSR analysis. CaO nanoparticles is used to determine whether a shooting was unintentional, committed in self-defense or with the intent to kill a person (Sermon et al. 2012). The distance from which the weapon is fired, and how close it comes to the target, is determined by the Global System for Standardization's (GSR) Common Sense Rating (CSR) system (Schwoeble and Exline 2000). Nanotechnology is the key to overcoming the drawback faced by conventional methods for determining global temperature (GSR) and other important information. The conventional methods used for GSR determination is very time-consuming and also not accurate.

Using the ancient method, the information remains unanalyzed (Meng and Caddy 1997). This approach involves the rearrangement of GSR using high-resolution scanning electron microscopy (HR-SEM) images (Pandya and Shukla 2018). An X-ray spectrometer in conjunction with a scanning electron microscope is useful for determining the chemicals present. The most accurate GSR analysis uses several nanodevices and nanomaterials, such as gold nanoparticles (Srividya 2016). Due to the high surface-to-volume ratio, it is possible to create ultrasensitive nano sensors that can detect as little as a few micrograms of the sample (Taudte et al. 2016).

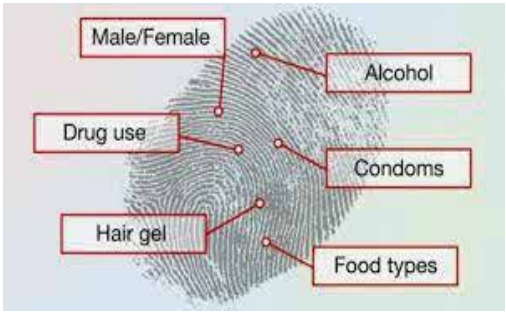



## 10. Forensic Fingerprint Development

The method of gathering evidence in rape crimes is frequently a simple, sensitive, and effective powder for fingerprint detection. Since the latter part of the nineteenth century, biometric identification of people has been done by using their fingerprints' distinctive patterns. One of the best systems for the safety and security of papers, gadgets (such phones, laptops, etc.), bank lockers, entrance control of workplaces, and forensic application in crime scene investigation is the development, identification, and presentation of the fingerprint (Wang et al., 2017).

## 11. Traditional Methods For Fingerprint Development

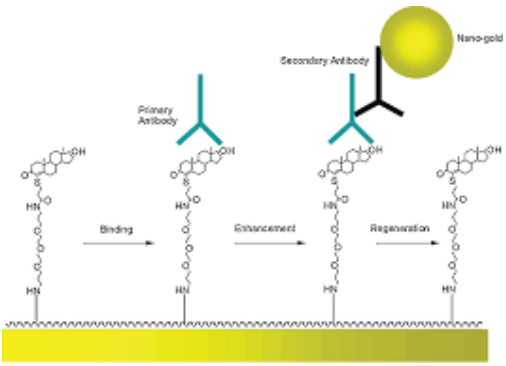
Finger prints left at crime scenes are one of the tools used to incriminate or eliminate suspects. The fingerprint showed the addition of CaO nanoparticles can be classified into three classes, patent prints, plastic prints, and latent prints. The patent prints are already visible to the naked eye because of blood, or through blood-covered fingers, or in ink or dirt. Plastic prints are left on a pliable surface consisting of clay or wax. Latent prints are left on surfaces due to the natural oils and sweat secreted from the skin. Two methods can perform fingerprint detection, one is the "physical method" (powder dusting) and the "chemical method". Traditional fingerprint powder composition is complexes of regular, luminescent, metallic, and thermoplastic powders (Exline et al., 2003).




## 12. Biosensors

A biosensor is the most efficient and multifaceted technology that plays a very indispensable role in the province of forensic sciences. Both forensic analysis and forensic investigation are fundamental branches of the modern analytical chemistry with a social security and legal implication, according to the American Chemi-

cal Society (ACS) (Ganesh 2016). Biosensors are most extensively used in the forensic toxicological analysis of different compounds and chemicals such as poisons, alcohol, toxins, and illicit drugs. Chemical and biological weapons and explosives can also be detected with the help of these biosensors. Nanotechnology have made a tremendous change in forensic investigations of addition CaO nanoparticles in biosensors are multifunctional and thus play an important role in forensic investigations. The use of biological sensing material on the nano-wafer or nano- substrate makes the biosensors more sensitive with enhanced performance. DNA sensors having DNA attached to the electrode are used for the detection of different poisons (Frederickx, Verheggen, & Haubruge, 2011).




## 13. Pre-blast and Post-Blast Identification

Explosives are any solid, liquid, or gaseous object capable of conducting a spontaneous chemical reaction is an explosive. Explosive detection is crucial in forensics since most explosives are used for malicious purposes, terrorism, or mass destruction (Cowan & Koppl, 2011).

Explosives are mainly classified into two, which are as follows:

- High explosive
- Low explosive

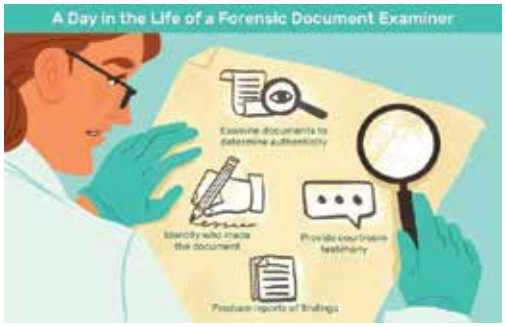
Explosives used in bombing attacks are mostly high explosives. High explosives are further classified as military, commercial, and improvised explosives. Military explosive is the chemical or mixture used in military, e.g. TNT, RDX, and PETN. Commercial explosives are chemical mixtures chemically used and produced such as ammonium nitrate/fuel oil (ANFO) (Trimpe). Micro-trace taggant technology can be used to identify and track cap-sensitive high explosives, such as cartridge-packed dynamite water gels and boosters. Pre-blast identification tags are discovered during the pre-blast recovery of an illegal explosive device. Use of explosives illicitly and the execution of criminal bombing cases can be simply understood using this technology (Seman et al. 2019). In addition of CaO nanoparticles explosives used in terrorist attacks are identified post-blast using identification taggants. Taggants are created by swapping out a hydrogen atom from a liquid or gas molecule. Isotropic technology is used for the purpose of uniquely identifying a detracted isotope. As a result, the potential of terrorism and mass destruction has decreased thanks to the widespread usage of taggants for explosive and dynamite identification (Karim et al. 2014).

## 14. Currency Identification

A crucial area to focus on is currency's security and distinctiveness. Numerous chemical and nano spectroscopic taggants are utilised to ensure the currency's uniqueness and prevent fraud (Natan et al. 2007). Since the spectroscopic taggants implanted in money notes are unique and cannot be duplicated, the original currency can be recognised. Additionally, invisible chemical and nanotaggants that are impossible to remove or duplicate are implanted in the currency. Therefore, taggants are widely used for the originality and security of the currency (Mead et al. 2014).

## 15. Document Identification

The security of anti-counterfeiting documents depends on tangential technologies as well. Important papers and documents are physically marked with taggants to monitor stolen or lost documents and to prevent duplication (Duong et al. 2014). Taggants are the unique technologies used for anti-counterfeiting and security document protection. The inks used in the printing or writing of important legal documents can be tagged with special micro-taggants. A tracker like physical taggant can be inserted on the document to save it from duplication and can be recovered when lost (Gooch et al. 2016a).

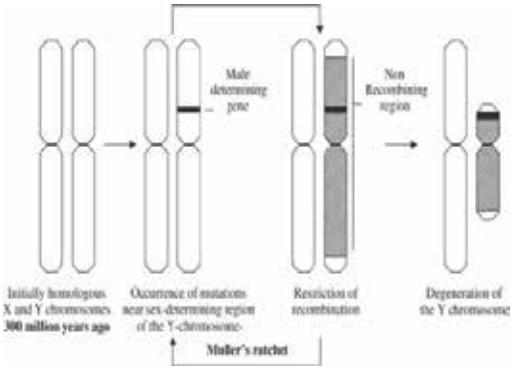



## 16. DNA Analysis

Nanotechnology can be an important tool for preventing crimes and for prosecuting offenders. DNA may now be extracted using magnetic nanoparticles from a variety of biological sources. One of the most crucial pieces of supporting evidence is the presence of an individual at the crime scene, regardless of whether their DNA belongs to the victim or the offender. Nowadays, magnetic CaO nanoparticles are being used to extract DNA from different biological sources like the blood, hair, skin, semen, and saliva (Eisenstein et al., 2011). Additionally, by creating nanotechnology-based instruments that can be used to directly read the DNA sequence in a molecule, more progress is made in the field of DNA analysis (McCord., 2006). Moreover, the DNA sequence can be examined using atomic force microscopy by mounting the DNA molecules on carbon nanotubes (Daniels et al., 2006).

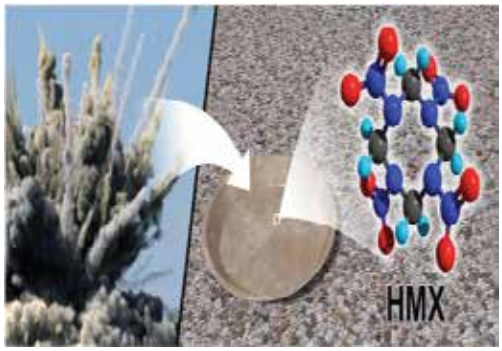
## 17. Y- Chromosomes Analysis

The issue of rape has been the central concern because it adversely impacts the health of exploited people by resulting in various illnesses, bodily injuries, sexual and reproductive problems, and mental clutter. It is based on four different sources of information. information obtained from the police, the general public through reviews, a legal DNA inquiry, and the judicial system. The Y chromosome is only found in men and is inherited from parents. It is passed down from a father to his child and can convey information from a male line that denotes the child to his father. In a mixture of male and female DNA samples, the study of genetic markers on the Y chromosome can specifically identify male evidence of sexual assault. Additionally, it could be applied to cases of sexual assault (Tilley & Ford, 1996).




## 18. Explosive Residue Detection

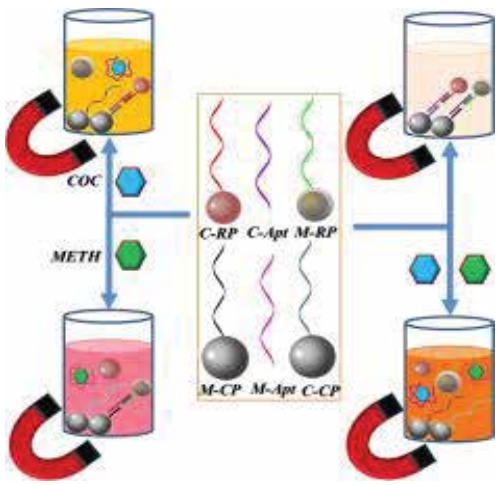
Nanotechnology can be used to identify minute quantities of shattered explosives at the time of crime scene analysis. The detection of trace amounts of explosive is a difficult undertaking because of many issues like minuscule quantities of an unexplored substance and contaminated samples, such as contaminated soil and water. Nano-based devices can be used to detect trinitrotoluene (TNT) up to 1nm level in aqueous solution in a turmeric extracted curcumin and CaO nanoparticles-based, highly selective, and ultrasensitive fluorescent probe. For superior results, when the examiner is unable to provide enough evidence and cannot find the unregimented parts of an explosive, the nanotechnology could be used (Pandya and Shukla 2018). The trace explosive detection also involves the collection of vapor and particulate systems and detecting them using the sensitive nanomaterials. There are significant advantages of nanotechnology-based sensors such as low cost, high sensitivity and low-consumption of power. Using nanotechnology, the explosive residue detection has become an easier and effortless task (Beveridge, 1992).




## 19. Illicit Drug Detection

Ilicit drugs can be used to commit crimes such as sexual harassment, rape, burglary, and robbery. The main motive of this crime is to impede the behavior, interpretation capability, or commandment ability of the person under the influence of a drug. Detection of illicit drugs is an important task as DFC includes dangerous crimes like sexual harassment and rape (Zhai et al. 2014). Forensic experts have a

difficult time detecting drugs because they are not present in the sample that was sent to the forensic laboratory for the inquiry in their original form. There are numerous drawbacks to the conventional method of drug testing, including cost effectiveness, instrument limitations, and instrument sensitivity, making application of nanotechnology in the pharmaceutical business vital for drug analysis. Nanotechnology and nanomaterials possess unique physicochemical properties along with the cost-effectiveness, capacity of miniaturization, and adaptability with compatibility that play a major role in the detection of illicit drugs. Research has proved that cocaine in the fingerprints can be determined using gold nanoparticles. Nanotechnology has made illicit drug detection a real-time easy job. A pin-sized gadget can be dipped in the saliva at the crime spot and can confirm the presence and absence of drugs. Also, alcohol analyzer used for drug testing can also be modified using this technology (Lad et al. 2016).




## 20. Conclusion

A review of the scientific literature on nanotechnology has shown the importance of nanotechnology in the field of forensic science, with a focus on how it can be applied to crime scene analysis and forensics. Nanotechnology and taggant technology have many uses in forensic science inquiry and how it can advance forensic science concerns like evidence gathering and handling, sample analysis, and monitoring of products and unlawful activities are just some of the ways in which nanotechnology is used in the field. Nanotechnology is an emerging field in which nanomaterials are developed that possess unique electrical, optical, and magnetic properties that can be applied to a wide range of forensic applications. These include evidence handling, fingerprint identification, illicit drugs, GSR, and explosives detection. Taggants are used in taggant technology, which enables continuous monitoring of these technologies, which can be advantageous and productive in preventative forensic and precautions. However, the real-world outlook for the application of such technology is still dismal. This can be the result of ignorance of such techniques or reluctance to adopt new technologies. Taggant technology has the ability to prevent a crime from occurring due to their continuous monitoring, while nanotechnology is capable of handling the repercussions of a crime scene. Together, these technologies will bring a revolution in various field of forensic science such as ballistics, fingerprint analysis, DNA analysis, Illicit Drug Detection and toxicology.

## 21. Reference


1. Abraham, S., & Sarathy, V. J. I. J. P. S. R. R. (2018). Biomedical applications of calcium oxide nanoparticles-a spectroscopic study. *49*(1), 121.

2. Akhtar, M. S., Panwar, J., Yun, Y.-S. J. A. S. C., & Engineering. (2013). Biogenic synthesis of metallic nanoparticles by plant extracts. *1*(6), 591-602.

3. Bernardini, J., Cinelli, P., Anguillesi, I., Coltelli, M.-B., & Lazzeri, A. J. E. P. J. (2015). Flexible polyurethane foams green production employing lignin or oxypropylated lignin. *64*, 147-156.

4. Biswas, P., Wu, C.-Y. J. J. o. t. a., & association, w. m. (2005). Nanoparticles and the environment. *55*(6), 708-746.

5. Brito, J. O., Silva, F., Leão, M., & Almeida, G. J. B. t. (2008). Chemical composition changes in eucalyptus and pinus woods submitted to heat treatment. *99*(18), 8545-8548.

6. Choi, Y. H., & Han, H.-K. J. J. o. P. I. (2018). Nanomedicines: current status and future perspectives in aspect of drug delivery and pharmacokinetics. *48*(1), 43-60.

7. Cunill, O. M., Salvá, A. S., Gonzalez, L. O., & Mulet-Forteza, C. J. I. J. o. H. M. (2019). Thirty-fifth anniversary of the International Journal of Hospitality Management: A bibliometric overview. *78*, 89-101.

8. Ealia, S. A. M., & Saravanakumar, M. (2017). *A review on the classification, characterisation, synthesis of nanoparticles and their application.* Paper presented at the IOP conference series: materials science and engineering.

9. Eram, R., Kumari, P., Panda, P. K., Singh, S., Sarkar, B., Mallick, M. A., & Verma, S. K. J. J. o. N. (2021). Cellular investigations on mechanistic biocompatibility of green synthesized calcium oxide nanoparticles with Danio rerio. *2*(1), 51-62.

10. Gross, L., Mohn, F., Moll, N., Schuler, B., Criado, A., Guitián, E., Peña, D., Gourdon, A., & Meyer, G. J. S. (2012). Bond-order discrimination by atomic force microscopy. *337*(6100), 1326-1329.

11. Halim, S., Mohamed, S., Azhan, H., Khawaldeh, S., & Sidek, H. J. P. C. S. (1999). Effect of barium doping in Bi–Pb–Sr–Ca–Cu–O ceramics superconductors. *312*(1-2), 78-84.

12. Holister, P., Weener, J.-W., Roman, C., & Harper, T. J. T. w. p. (2003). Nanoparticles. *3*, 1-11.

13. Hulkoti, N. I., Taranath, T. J. C., & Biointerfaces, s. B. (2014). Biosynthesis of nanoparticles using microbes—a review. *121*, 474-483.

14. Iravani, S. (2011). Green synthesis of metal nanoparticles using plants. *Green Chemistry, 13*(10), 2638-2650.

15. Kumar, V., Kumar, S., Chauhan, P., Verma, M., Bahuguna, V., Joshi, H. C., Ahmad, W., Negi, P., Sharma, N., & Ramola, B. J. S. r. (2019). Low-tempera-

ture catalyst based hydrothermal liquefaction of harmful macroalgal blooms, and aqueous phase nutrient recycling by microalgae. *9*(1), 1-9.

16. Marquis, G., Ramasamy, B., Banwarilal, S., Munusamy, A. P. J. J. o. P., & Biology, P. B. (2016). Evaluation of antibacterial activity of plant mediated CaO nanoparticles using Cissus quadrangularis extract. *155*, 28-33.

17. Mody, V. V., Nounou, M. I., & Bikram, M. J. A. d. d. r. (2009). Novel nanomedicine-based MRI contrast agents for gynecological malignancies. *61*(10), 795-807.

18. Mohammadian, M., Abasi, E., Akbarzadeh, A. J. A. c., nanomedicine,, & biotechnology. (2016). Mesenchymal stem cell-based gene therapy: A promising therapeutic strategy. *44*(5), 1206-1211.

19. Moreno-Olivas, F., Gant, V. U., Johnson, K. L., Peralta-Videa, J. R., & Gardea-Torresdey, J. L. J. J. o. Z. U. S. A. (2014). Random amplified polymorphic DNA reveals that TiO2 nanoparticles are genotoxic to Cucurbita pepo. *15*(8), 618-623.

20. Mustafa, G., Tahir, H., Sultan, M., & Akhtar, N. J. A. J. o. B. (2013). Synthesis and characterization of cupric oxide (CuO) nanoparticles and their application for the removal of dyes. *12*(47), 6650-6660.

21. Nunthavarawong, P., Sanjay, M., Siengchin, S., & Thoppil-Mathew, M. (2022). Introduction to Antimicrobial and Antiviral Materials *Antimicrobial and Antiviral Materials* (pp. 1-4): CRC Press.

22. Patel, K., Szabo, S., & Hemandez, V. J. H. p. (2008). protuberans COL1A1-PDGFB fusion is identified in virtually all protuberans cases when investigated by newly developed multiplex reverse transcription polymerase chain reaction and fluorescence in situ hybridization assays. *39*(2), 184.

23. Ranghar, S., Sirohi, P., Verma, P., Agarwal, V. J. B. A. o. B., & Technology. (2014). Nanoparticle-based drug delivery systems: promising approaches against infections. *57*, 209-222.

24. Roco, M. C. (2011). The long view of nanotechnology development: the National Nanotechnology Initiative at 10 years *Nanotechnology research directions for societal needs in 2020* (pp. 1-28): Springer.

25. Roco, M. C., Mirkin, C. A., & Hersam, M. C. (2011). Nanotechnology research directions for societal needs in 2020: retrospective and outlook.

26. Salari, M., Amine, G., Shirazi, M., Hafezi, R., Mohammadypour, M. J. C. M., & Infection. (2006). Antibacterial effects of Eucalyptus globulus leaf extract on pathogenic bacteria isolated from specimens of patients with respiratory tract disorders. *12*(2), 194-196.

27. Sinha, S., Aman, A. K., Singh, R. K., Kr, N., & Shivani, K. J. M. T. P. (2021).

Calcium oxide (CaO) nanomaterial (Kukutanda twak Bhasma) from egg shell: Green synthesis, physical properties and antimicrobial behaviour. *43*, 3414-3419.

28. Vecchio, M. G., Loganes, C., & Minto, C. J. T. O. A. J. (2016). Beneficial and healthy properties of Eucalyptus plants: A great potential use. *10*(1).

29. Daniels, L. B., Clopton, P., Bhalla, V., Krishnaswamy, P., Nowak, R. M., McCord, J., . . . Storrow, A. B. J. A. h. j. (2006). How obesity affects the cut-points for B-type natriuretic peptide in the diagnosis of acute heart failure: results from the Breathing Not Properly Multinational Study. *151*(5), 999-1005.

30. Eisenstein, D. J., Weinberg, D. H., Agol, E., Aihara, H., Prieto, C. A., Anderson, S. F., . . . Balbinot, E. J. T. A. J. (2011). SDSS-III: Massive spectroscopic surveys of the distant universe, the Milky Way, and extra-solar planetary systems. *142*(3), 72.

31. Le, M., Raxworthy, C. J., McCord, W. P., Mertz, L. J. M. p., & evolution. (2006). A molecular phylogeny of tortoises (Testudines: Testudinidae) based on mitochondrial and nuclear genes. *40*(2), 517-531.

32. Tilley, N., & Ford, A. (1996). *Forensic science and crime investigation*: Home Office, Police Research Group London.

33. Beveridge, A. J. F. s. r. (1992). Development in the Detection and Identification of Explosive Residues. *4*(1), 17-49.

34. Beveridge, A. J. F. s. r. (1992). Development in the Detection and Identification of Explosive Residues. *4*(1), 17-49.

35. Cowan, E. J., & Koppl, R. J. T. R. o. A. E. (2011). An experimental study of blind proficiency tests in forensic science. *24*(3), 251-271.

36. Daniels, L. B., Clopton, P., Bhalla, V., Krishnaswamy, P., Nowak, R. M., McCord, J., . . . Storrow, A. B. J. A. h. j. (2006). How obesity affects the cut-points for B-type natriuretic peptide in the diagnosis of acute heart failure: results from the Breathing Not Properly Multinational Study. *151*(5), 999-1005.

37. Eisenstein, D. J., Weinberg, D. H., Agol, E., Aihara, H., Prieto, C. A., Anderson, S. F., . . . Balbinot, E. J. T. A. J. (2011). SDSS-III: Massive spectroscopic surveys of the distant universe, the Milky Way, and extra-solar planetary systems. *142*(3), 72.

38. Exline, D. L., Wallace, C., Roux, C., Lennard, C., Nelson, M. P., & Treado, P. J. J. J. o. f. s. (2003). Forensic applications of chemical imaging: latent fingerprint detection using visible absorption and luminescence. *48*(5), 1047-1053.

39. Frederickx, C., Verheggen, F., & Haubruge, E. J. B., Agronomie, Société et Environnement. (2011). Biosensors in forensic sciences. *15*(3).

40. Tilley, N., & Ford, A. (1996). *Forensic science and crime investigation*: Home Office, Police Research Group London.

41. Trimpe, M. The Current Status of GSR Examinations| FBI: Law Enforcement Bulletin (2022).

42. Wang, M., Li, M., Yu, A., Zhu, Y., Yang, M., & Mao, C. J. A. f. m. (2017). Fluorescent nanomaterials for the development of latent fingerprints in forensic sciences. *27*(14), 1606243.

Seyda Mona *et al.LGU (IJECI) 2022*

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

LGU International Journal for
**Electronic Crime Investigation**

Research Article

Vol. 6 issue 2 Year 2022

# Nanotechnology: An applied and extensive approach in solving crimes

**Dr. Syeda Mona Hassan[1] and Dr. Aftab Ahmad Malik[2]**
[1] Department of Chemistry, University of agriculture, Faisalabad
[2] Faculty of Computer Sciences and Engineering, Ghulam Ishaq Khan Institute of Science and Engineering, KPK

## Abstract:

Nanotechnology has great influence on modern technology. In order to identify, individualize, and assess evidence, forensic science applies knowledge and methods. Then, with the aid of evidence, crime scenes will be rebuilt, investigations will be directed, and offenders will be prosecuted. Nano-analysis is one of modern technology that is most frequently used in forensic science. The characterization can be done by using tools like the atomic force microscope (AFM), aman micro spectroscopy, scanning electron microscope (SEM), and transmission electron microscope (TEM) (Micro-Raman). Nanotechnologies might be essential in current forensic investigation issues like forensic toxicological analysis, explosive detection, detection of explosive residue, finger print analysis, forensic DNA analysis, forensic nano trackers, and drug-facilitated crime.

**Key words:** Nanotechnology, Security purposes, Drug facilitated crime, Explosive weapons.

## 1. Introduction

The topic of nanotechnology is rapidly expanding and opens up new avenues for research and technology. Electronics, engineering, physical sciences, materials sciences, health sciences, and many other scientific domains have all used it. Forensic science and society stand to gain greatly from nanotechnology, yet those nanoparticles with novel undiscovered qualities can also be hazardous to the environment (Chauhan, Singh, & Tiwari, 2017). An essential benefit of adopting nanotechnology in forensic science is that it makes hidden evidence visible, which can help the forensic scientists conclude their investigations (Chen, 2011). With the aid of new scientific techniques like microbial forensics, forensic science, and nanotechnology, the novel methods that were used in the past or are still used today for investigating a crime scene can be replaced. Examples include the smidgen method that was used to reveal finger prints or the use of fluorescent x-ray tubes (Pandya & Shukla, 2018). In the field of forensic sciences, the application of cutting-edge nanotechnology technology can help in investigation (Bhatt, Pandey, Tharmavaram, Rawtani, & Mustansar Hussain, 2020).

Nanotechnology is useful with the creation and solicitation of organizationally-featured arrangements and devices within a scale of around 100 nm, where unique properties emerge in contrast to bulk materials. It means the ability to manipulate molecules and atoms to create customized nanostructures and gadgets for specific purposes. This is due to the merging of science in the fields of materials science, biology physics, chemistry, and engineering at the Nano scale as well as the significance of matter control in nearly all technologies (Hulla et al., 2015).

Chemical or biological methods can be used to create nanoparticles. Due to the presence of some harmful chemicals absorbed on the surface, chemical manufacturing processes have been linked to numerous negative effects. Biological techniques of nanoparticle manufacturing involving microbes, fungi, plants or plant extracts and enzymes are eco-friendly alternatives to physical and chemical approaches. $Fe_3O_4$ (magnetite) and FeO (maghemite), are two types of magnetic nanoparticles. They have been actively analyzed for guided medication administration, gene therapy, magnetic resonance imaging (MRI), targeted cancer treatment (magnetic hyperthermia) and DNA analysis (Hasan, 2015).

Nanotechnology, which eventually raises the risk to human health and the environment. There has been a rise in interest in creating ecologically friendly processes for creating metallic nanoparticles. A useful strategy in green nanotechnology is the utilization of various biomaterials for the creation of nanoparticles. Metallic nanoparticles that are energy-efficient, nontoxic, inexpensive and beneficial to the environment have been produced using biological resources like bacteria, algae, fungi, and plants. An overview of numerous studies on iron oxide ($FeO/Fe_3O_4$) and zero valent metallic iron (ZVMI) nanoparticles illustrates its important uses in reducing environmental pollution (Saif, Tahir, & Chen, 2016).

## 2. Iron Oxide Nanoparticles

Iron oxides are typical natural substances that are also simple to create in a laboratory. Including oxides, hydroxides, and oxide-hydroxides, there are 16 different types of iron oxide. These minerals are the end product of aqueous reactions occurring in a variety of redox reactions (Campos et al., 2015).

Iron oxide nanoparticles, which have sizes between 1 and 100 nanometers and are used in drug administration, magnetic data storage and bio-sensing. The surface area to volume ratio greatly rises in nanoparticles (NPs). This enables NPs to have a superior dispersibility in solutions and a significantly larger binding capacity. Super paramagnetism is a property of magnetic NPs with diameters ranging from 2 to 20 nm, which indicates that they are externally magnetizable and have a magnetization of zero in the absence of a magnetic field (Palanisamy & Wang, 2019).

## 3. Synthesis and Characterization of Iron Oxide Nanoparticles

Iron oxides typically consist of a surface layer and a crystalline core that stabilizes the core's characteristics and may also be used to avoid aggregation. The process of synthesizing the iron oxide's crystalline core, which is composed of ferro- ($Fe^{2+}$) or ferri- ($Fe^{3+}$)

magnetic material, often involves the precise precipitation of iron oxides in an aqueous solution or an organic solution while also incorporating a base. Due to their polymorphism involving temperature-induced phase transition, the three most widely used iron oxides are hematite (-$Fe_2O_3$), maghemite (-$Fe_2O_3$), and magnetite ($Fe_3O_4$). These minerals have special catalytic, magnetic, biochemical and other properties that make them suitable for particular technical and biomedical uses (Sangaiya, Jayaprakash, & Magnetism, 2018).

For the creation of monodispersed nanoparticles, an effective synthetic method relies on the breakdown of organometallic precursors. This process produces iron oxide nanoparticles (magnetite/maghemite $Fe_3O_4$/-FeO). Typically, the maximum particle size for this approach was between 20 and 30 nm (Guardia, Pérez, Labarta, & Batlle, 2010).

The FT-IR (Fourier transform infrared spectroscopy), UV absorption spectroscopy, XRD (X-ray diffractometer), EDX (Energy Dispersive X-Ray spectrometer), and SEM (scanning electron microscope) were used to characterize the biosynthesized iron oxide nanoparticles. The forms were crystalline, Nanorod, and enormously stable, and the typical particle size was between 10 and 20 nm. (Rajiv, Bavadharani, Kumar, Vanathi, & Biotechnology, 2017).

## 4. Applications of nanotechnology in criminology

Fingerprint analysis

Since the beginning of time, criminologists have employed fingerprints as a distinctive form of evidence. Particularly useful in fingerprint analysis is nanotechnology. The use of considerably smaller nanoparticles in place of traditional materials like carbon black, aluminium flake, and gentian violet has greatly increased the sensitivity of the fingerprinting process. Even on complex surfaces like adhesive or textured materials, the nanoparticles are making it simpler to find and remove fingerprints that have been left behind (Prasad, Lukose, & Prasad, 2016). Nanotechnology is also being used to instantly and precisely disclose hidden fingerprints. Even on a damaged and faded print, the nanoparticles can enhance the fingerprints by adhering to the ridges and grooves (Pitkethly, 2009). In addition to the patterns, the fingerprint also contains the person's sweat and other metabolites. The nanoparticles are able to show whether the owner of the fingerprint is a cocaine addict or an alcoholic by attaching to such body fluids and metabolites infused in the print. They are also able to reveal his age, sex, and the ailments he would undoubtedly suffer from (Pandya & Shukla, 2018).

Fingerprint analysis

## 5. Atomic Force Microscope (AFM)

The Atomic Force Microscope (AFM) is an

instrument that forensic experts use to examine the paper's surface at the nanoscale. The investigator can use this information to identify whether the document is a counterfeit or was actually written by one or more people by knowing the pen, ink, and pressure/intensity. By disclosing the blood sample's age, AFM helps the investigating officer look into body offences. Over time, blood thickens and stiffens (Pandey, Tharmavaram, Rawtani, Kumar, & Agrawal, 2017). AFM can reveal the sample's age by measuring the viscosity or dryness of the sample. The detective is receiving assistance from AFM in identifying the compounds found in the urine. When urine is combined with nanoparticles and exposed to laser light, a signal is released that indicates the presence of chemicals or other things, such as pharmaceuticals, in the urine (Yadavalli & Ehrhardt, 2021).

## 6. DNA Analysis

The advancement and improvement of DNA analysis looks to be the most promising use of nanotechnology. DNA may now be extracted, amplified, separated, and sequenced more quickly and conveniently thanks to nanotechnology (Moller & Fritzsche, 2007). In addition to revealing the physical characteristics of the owner of the DNA, such as age, sex, and the colour of the hair, eyes, and skin, among other things, next-generation sequencing using nanotechnology is also assisting the detective in determining the origin of DNA, including whether the DNA lifted from the crime scene came from skin, blood, saliva, semen, etc (Kaur & Sharma, 2022).

DNA Analysis

## 7. Explosives Weapons

Explosives and weapons with explosive components are now frequently used by terrorists and in terrorist occurrences (Wang, 2004). Investigators can employ nanotechnology to determine the amount of intact or barely fragmented explosives at the crime scene during the course of the inquiry. Once more, nanotechnology is demonstrating its efficacy in the evaluation and detection of gunshot residue (Sree Satya Bharati, Byram, & Soma, 2018)

## 8. Nanotrackers

These days, using trackers and bar codes has become commonplace. Trackers can assist in locating lost or stolen objects. Nano trackers are also employed to keep convicts from breaking the law and to keep tabs on them after their release. Inmates that receive nano tracker injections are quite easy to find (Singh & Samal, 2021).


Nanotrackers

## 9. Forged Products (set-up)

Nanotechnology is also helping differentiate false products from originals. Police are able to detect crimes involving inauthentic aspects by using nanofibers and nanodots. Bio-Nanosensors are also being used to identify toxins and to detect narcotics, explosives and bioterrorist agents (Mandal & Mandal, 2015).

Forged Product Investigation

## 10. Security purposes

By lowering the time, expense, and level of skill needed while simultaneously improving the precision and accessibility of nano collecting and analysis devices, nanotechnologies in forensic science and security can revolutionize the way an investigation is conducted (Muro, Doty, Bueno, Halamkova, & Lednev, 2015).

Forensic investigation for security purposes

## 11. Conclusion

With distinctive qualities, nanotechnology have many uses in forensic science like evidence gathering and handling, sample analysis, and monitoring of products and unlawful activities. Utilizing nanomaterials with special electrical, optical, and magnetic properties allows for a wide range of forensic applications, including the processing of evidence, fingerprint recognition, the detection of illegal narcotics, explosives, and GSR.

## 12. References

1. Hulla, J., Sahu, S., Hayes, A. J. H., & toxicology, e. (2015). Nanotechnology: History and future. 34(12), 1318-1321.

2. Hasan, S. J. R. J. R. S. (2015). A review on nanoparticles: their synthesis and types. 2277, 2502.

3. Saif, S., Tahir, A., Asim, T., & Chen, Y. J. N. (2016). Plant mediated green synthesis of CuO nanoparticles: comparison of toxicity of engineered and plant mediated CuO nanoparticles towards Daphnia magna. 6(11), 205.

4. Guardia, P., Pérez, N., Labarta, A., & Batlle, X. J. L. (2010). Controlled synthesis of iron oxide nanoparticles over a wide size range. 26(8), 5843-5847.

5. Rajiv, P., Bavadharani, B., Kumar, M. N., Vanathi, P. J. B., & Biotechnology, A. (2017). Synthesis and characterization of biogenic iron oxide nanoparticles using green chemistry approach and evaluating

their biological activities. 12, 45-49.

6. Sangaiya, P., Jayaprakash, R. J. J. o. S., & Magnetism, N. (2018). A review on iron oxide nanoparticles and their biomedical applications. 31(11), 3397-3413.

7. Campos, E. A., Pinto, D. V. B. S., Oliveira, J. I. S. d., Mattos, E. d. C., Dutra, R. d. C.

8. L. J. J. o. A. T., & Management. (2015). Synthesis, characterization and applications of iron oxide nanoparticles-a short review. 7, 267-276.

9. Palanisamy, S., & Wang, Y.-M. J. D. t. (2019). Superparamagnetic iron oxide-nanoparticulate system: synthesis, targeting, drug delivery and therapy incancer.48(26), 9490-9515.

10. Sangaiya, P., Jayaprakash, R. J. J. o. S., & Magnetism, N. (2018). A review on iron oxide nanoparticles and their biomedical applications. 31(11), 3397-3413

11. Andrews, D. P. NAME 2021 Recap!

12. Bhatt, P. V., Pandey, G., Tharmavaram, M., Rawtani, D., & Mustansar Hussain, C. (2020). Nanotechnology and Taggant Technology in Forensic Science. Technology in Forensic Science: Sampling, Analysis, Data and Regulations, 279-301.

13. Boumba, V. A., & Vougiouklakis, T. (2015). Impact of blood collection tubes on erroneous 1-propanol detection and on forensic ethanol analysis. J Forensic Toxicol Pharmacol, 4(1).

14. Campos, E. A., Pinto, D. V. B. S., Oliveira, J. I. S. d., Mattos, E. d. C., Dutra, R. d. C. L. J. J. o. A. T., & Management. (2015). Synthesis, characterization and applications of iron oxide nanoparticles-a short review. 7, 267-276.

15. Chauhan, V., Singh, V., & Tiwari, A. (2017). Applications of nanotechnology in forensic investigation. Int. J. Life. Sci. Scienti. Res, 3(3), 1047-1051.

16. Chen, Y. f. (2011). Forensic applications of nanotechnology. Journal of the Chinese Chemical Society, 58(6), 828-835.

17. Kaur, L., & Sharma, S. G. (2022). Forensic DNA Analysis: A Powerful Investigative Tool Crime Scene Management within Forensic Science (pp. 1-40): Springer.

18. Mandal, S., & Mandal, M. (2015). Can Bacteria Subsist on Antibiotics. J Forensic Toxicol Pharmacol, 4(2).

19. Moller, R., & Fritzsche, W. (2007). Metal nanoparticle-based detection for DNA analysis. Current Pharmaceutical Biotechnology, 8(5), 274-285.

20. Muro, C. K., Doty, K. C., Bueno, J., Halamkova, L., & Lednev, I. K. (2015). Vibrational spectroscopy: recent developments to revolutionize forensic science. Analytical chemistry, 87(1), 306-327.

21. Palanisamy, S., & Wang, Y.-M. J. D. t. (2019). Superparamagnetic iron oxide nanoparticulate system: synthesis, targeting, drug delivery and therapy in cancer.

48(26), 9490-9515.

22. Pandey, G., Tharmavaram, M., Rawtani, D., Kumar, S., & Agrawal, Y. (2017). Multifarious applications of atomic force microscopy in forensic science investigations. Forensic science international, 273, 53-63.

23. Pandya, A., & Shukla, R. K. (2018). New perspective of nanotechnology: role in preventive forensic. Egyptian Journal of Forensic Sciences, 8(1), 1-11.

24. Pitkethly, M. (2009). Nanotechnology and forensics. Materials Today, 12(6), 6.

25. Prasad, V., Lukose, S., & Prasad, L. (2016). Emerging forensic applications of nanotechnology. Int J Eng Allied Sci, 2, 1-8.

26. Sangaiya, P., Jayaprakash, R. J. J. o. S., & Magnetism, N. (2018). A review on iron oxide nanoparticles and their biomedical applications. 31(11), 3397-3413.

27. Singh, S., & Samal, N. (2021). Nanotechnology: A Powerful Tool in Forensic Science for Solving Criminal Cases. Arab Journal of Forensic Sciences & Forensic Medicine, 3(2), 273-296.

28. Sree Satya Bharati, M., Byram, C., & Soma, V. R. (2018). Femtosecond laser fabricated Ag@ Au and Cu@ Au alloy nanoparticles for surface enhanced Raman spectroscopy based trace explosives detection. Frontiers in Physics, 6, 28.

29. Wang, J. (2004). Microchip devices for detecting terrorist weapons. Analytica Chimica Acta, 507(1), 3-10.

30. Yadavalli, V. K., & Ehrhardt, C. J. (2021). Atomic force microscopy as a biophysical tool for nanoscale forensic investigations. Science & Justice, 61(1), 1-12.

# Editorial Policy and Guidelines for Authors

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

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

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

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

# LAHORE GARRISON UNIVERSITY

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

## VISION

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

## MISSION

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

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


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