The Emerging Technology in Cybercrime of Cyberspace: An Overview

Dr. Mukesh Kumar Chaurasia[1], Nishtha Thakur[2]

[1]Faculty, Department of Criminology and Forensic Science, Dr. Hari Singh Gour University Sagar MP
[2]PG Student, Department of Criminology and Forensic Science, Dr. Hari Singh Gour University Sagar MP

ABSTRACT

Cyber criminology and Cyberspace are closely related aspects; hence, Cyberspace provides an environment where Cyberspace occurs. Cyberspace is a domain that in the rapid increase in technology signifies how digital platforms are vulnerable for securing data and privacy of an individual, which causes various crimes in the world. Cyberspace is known as organized criminal attacks on Cybersecurity and Cyberspace through attacks, Hacking, Bullying, etc. Cybersecurity and information security are essential and unavoidable components of using the internet or digital places. Numerous types of standards, protocols, policies, technologies, and antiviruses have been developed to protect data and privacy. To ensure that technology is increasing as security, privacy, and data taken as a liability, which is the main cause of Cybercrime.

This paper will enhance the emergence of technology in Cyber criminology and the necessity of Cybersecurity, how awareness of Cybersecurity should be known in our society, and what people need to know about Cybercrime. It also highlights Cyber-attacks occurring in organizations and institutions. This study focused on a qualitative data collection method from secondary data sources to increase the information and certainty of Cyber criminology in Cyberspace. The conclusions drawn in this paper are based on a study on this subject.

Keywords: Cybercrime, Cyberspace, Cybersecurity, Information security, Attacks.

1. INTRODUCTION

Cyber criminology is a term that signifies the relationship between crime and Cyberspace. Cyberspace is known by many fields of study, but criminology was too late to explore this space and address a new form of criminality called Cybercrime. Criminologist Kuruppannan Jaishankar founded Cyber criminology in 2007 and he defined in his journal that "the study of causation of crimes that occur in Cyberspace and its impact in the physical space". Hence, the relation between Cyber criminology and Cybersecurity is “Cybercrime’. Cybersecurity is an umbrella concept used by criminologists to refer to traditional crimes that are enhanced via the use of networked technologies (i.e. Cyber-enabled crimes) and newer forms of crime that would not exist without network technologies (i.e. Cyber-dependent crimes). While Cybersecurity is by itself a very broad concept and a diverse field of practice for computer scientists, the term ‘Cybersecurity’ typically refers to policies, processes, and practices undertaken to protect data, networks, and systems from unauthorized access. Cybersecurity is used in national security, organizations, government-healthcare institutions, the corporate world, and many other contexts to capture an increasingly diverse array of threats. Increasingly, Cybercrime is presented as a threat to Cybersecurity, which explains why security institutions are gradually becoming involved in Cybercrime control and prevention activities. Every year, Cyberspace and Cybersecurity threats are increasing with different kinds of activities; simultaneously, these crimes and threats are increasing with increasing complexity. Therefore, the primary purpose of Cybersecurity is to secure the data of individuals and institutions on the internet. In brief, Cybersecurity ensures the security of virtual life on Cyber networks.

The growth of technologies, infrastructures, and platforms with less or no security protection in emerging Artificial Intelligence (AI) and Machine Learning (ML) technologies and internet of things (IoT) trends increases the likelihood of Cyberspace attacks, which is why it is also called Computer crime. Cyberspace involves using computers as a weapon to commit fraud, trafficking in pornography and intellectual property, stealing identities, or violating privacy. Cyberspace is seen as a liability unless proper security is developed in it, which is based on antivirus software, protocols, and standards of Cybersecurity, which are based on ISO 27001/2~ISMS (Information Security Management System), NIST (National Institute of Standards and Technology) framework, GDPR (General Data Protection Regulation), and COBIT (Control Objectives for Information and Related Technology). Indeed, as technology progresses, Cyber criminals continuously evolve their methods and tactics to adapt to the changing digital landscape. The main aspect is the emerging technology of Cyberspace, which causes Cybercrime. Therefore, Cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not occur on a physical platform, they do occur on a personal or corporate virtual platform, which is the set of informational attributes that define people and institutions on the Internet.

The following are the primary aspects related to Cyber criminology within the context of Cyberspace;
Cyber Bullying is Bullying with the pervasive use of digital technologies such as social media, Artificial intelligence (AI) and digital tools like photoshop, there has been a profound impact on various aspects of communication, creativity, and information dissemination. It can occur on social media, messaging platforms, gaming platforms, and mobile phones. Repeated behavior aimed at scaring, angering, or shaming those who are targeted. Online Bullying, which includes the use of electronic devices and technology to send hurtful, threatening, or offensive messages, post malicious content, or engage in other harmful online activities with the intention of causing emotional distress, humiliation, or harm to the target. Cyber Bullying can take various forms, but not restricted to posting embarrassing images or videos, making disparaging remarks, disseminating untrue stories, and posing as someone else online, such as deepfake videos or photos. It can have serious consequences for the victims, leading to emotional and mental distress as well as potentially long-term effects on mental health.
In the field of criminology, Cyber-piracy and privacy concerns are topics of significant interest. **Cyber Piracy** refers to criminal activities conducted in the digital realm, often for financial gain, that involve the unauthorized acquisition, distribution, or use of intellectual property, digital assets, or proprietary information. **Privacy concerns** in criminology focus on issues related to the protection of personal information and the legal and ethical implications of privacy breaches.
Hackers are individuals who possess advanced computer skills and knowledge, which they use to explore and manipulate computer systems and networks. There are many types such as ethical hackers, gray hat and white hat hackers. A hacker is an information technology expert who uses non-traditional methods to accomplish objectives. It's crucial to remember that in legal situations, honest people can use Hacking.

But the word "hacker" has evolved to mean a security hacker in popular culture. These people are skilled in breaking into computers and taking advantage of security flaws in software to obtain data that is normally protected. Law enforcement organizations, for instance, use Hacking tactics to obtain evidence against criminals and other bad actors. White hat hackers are those who use anonymity techniques, such as a Virtual Private Network (VPN) or the dark web, to hide their identities online and pretend to be criminals for the sake of investigations.

Attackers are individuals or entities who engage in Cyberattacks with malicious intent, the term "attacker" generally refers to those engaged in malicious activities without permission or ethical justification.

Technology Infrastructure refers to the foundational framework of hardware, software, networks, data centers, and other components that support an organization's or a system's information technology (IT) needs. It is the backbone that enables the operation, management, and delivery of IT services and applications. Technology infrastructure plays a critical role in the functioning and efficiency of modern businesses, institutions, and digital systems.

Digital platforms are online environments or ecosystems that facilitate various activities, interactions, and transactions over the internet. These platforms provide a foundation for users, businesses, and developers to connect, share, and access digital content, services, or products.

2. Literature Review:

Enhancing Relationships between criminology and Cybersecurity~ By Benoît Dupont, Chad Whelan

Cybercrime is a growing threat involving networked technologies, affecting various contexts. It's often seen as a challenge to Cybersecurity, highlighting the need for increased engagement and ideas exchange. This approach views crime and security as part of a shared continuum, emphasizing collaboration between researchers in these fields. This integrated perspective explores the nuanced relationship between Cybercrime and Cybersecurity**.**

A Systematic Literature Review on the Cybersecurity~ By Dr. Yusuf Perwej et al

The primary objective of this article is to conduct a comprehensive analysis of various aspects of Cybersecurity, including the importance of Cybersecurity, the Cybersecurity framework, tools used in Cybersecurity, and the challenges it presents. Cybersecurity is the practice of safeguarding and recovering networks, devices, and programs from various forms of Cyberattacks.

A Comprehensive Review of Cybersecurity Vulnerabilities, Threats, Attacks, and Solutions~ By Ömer Aslan *at el*

Emerging technologies like cloud computing, IoT, and cryptocurrencies have raised Cybersecurity concerns. Traditional protection systems are ineffective against new-generation attacks. This paper explores reasons behind Cyber-attacks, recent incidents, and proposes innovative solutions to enhance Cybersecurity measures using trending technologies.

The Future of Cybercrime in Light of Technology Development~ By Jacopo Bellasio at El

This thorough study examines future technologies and their potential threats to Cybercrime, examines the impact of ICT (information communication technology) changes on Cyber-dependent and Cyber-enabled crimes, and proposes strategies to prevent their exploitation and understands the trending technologies.

3. Present Study-

Emerging technologies in the realm of Cybercrime refer to new and advanced tools, techniques, or methods that Cybercriminals adopt to exploit vulnerabilities and carry out malicious activities. The emergence of new technologies poses a potential threat to security, emphasizing the need for robust Cybersecurity measures. This thorough study provides an overview of current technology advancements-based solutions for Cybersecurity issues.

4. Objective of Study- The present study focuses on following objectives,

1. To identify and analyze emerging technologies in Cybercrime.
2. To examine the impact of emerging technologies on Cybersecurity.
3. To explore the technological foundation of Cybersecurity industry perspective.
4. To evaluate the ethical implications due to emerging technology.

5. Methodology- This study is founded on an analysis of specific research papers, providing an overview of the findings within the scope of this work, employs qualitative data collection methods, drawing from secondary sources, the purpose is to identify the future trends, challenges and opportunities in the field of technology and the requisite understanding of Cybersecurity.

6. DATA ANALYSIS

Cybercrimes occur due to lack of Cybersecurity, with 300,000 new malwares being created every day and Hacker attacks occur every 39 seconds, it is difficult for organizations to protect themselves entirely. The number of Cybercrime incidents exceeded 31,000 cases worldwide in 2019, and the global number of data breaches with confirmed data lost was almost 4000 that year. Approximately 2328 Cybercrimes are thought to occur each day, with an estimated loss of nearly $26 billion (about $80 per person in the US) (about $80 per person in the US) over the last 21 years from 2001 to 2021. In 2020, victims reported the top three crimes, with phishing scams, non-payment/non-delivery scams, and extortion ranking as the most frequently reported offenses. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Remarkably, in 2020, there was a notable increase in scams capitalizing on the circumstances surrounding the COVID-19 pandemic. The IC3 (Internet crime complaint center) received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals, Some of the Cybersecurity threats that are expected trends in 2023 are smart devices as a Hacking target, especially IOT devices that may have weak security or misuse by users. Phishing attacks, social engineering, cloud security attacks, supply chain attacks, and ransomware attacks are the most common attacks that we saw in 2023. India is the world's largest populated country, and billions of people need connectivity to the world through the Internet. While greater connectivity via the World Wide Web promises large-scale progress, it also leaves our digital society open to new vulnerabilities.

According to the National Crime Records Bureau (NCRB) report, Cybercrime incidents are reported to the law enforcement agencies of the respective states and Union Territories (UT). The data reveals that over 1.6 million Cybercrime incidents have been reported, leading to the registration of more than 32 thousand First Information Reports (FIRs) between January 1, 2020, and December 7, 2022. The government only generated these data; however, there are more statistics from other websites.

According to a survey, the number of Cyberattacks in India increased dramatically in the first three months of 2023. Industries Face discovered that most attacks in India were directed against the BFSI sector, particularly the insurance industry. Compared to the global average of 4%, 11% of all websites in the insurance business in India experienced an attack. Ninety-nine percent of attacks were vulnerability attacks such as botnet-based probe attacks, instead of distributed denial of service (DDoS) attacks like ransomware. Up until January 31, 2023, over 7 lakh complaints—including those from Odisha—have been filed through the Citizen Financial Cyber Fraud Reporting and Management System since its launch. In response to almost 1.90 lakh complaints, funds totaling more than Rs. 235 crores have been saved thus far. Over 52,000 grievances have been resolved.

To spread awareness on Cybercrime, the Central Government has taken initiatives that, inter-alia, include; dissemination of messages through SMS and I4C social media accounts. Twitter handle (@Cyberdost), Facebook (CyberDostI4C), Instagram (Cyberdosti4c), Telegram (Cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple media, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to perform publicity to create mass awareness.

7. Emerging technology that use in Cyber Crime

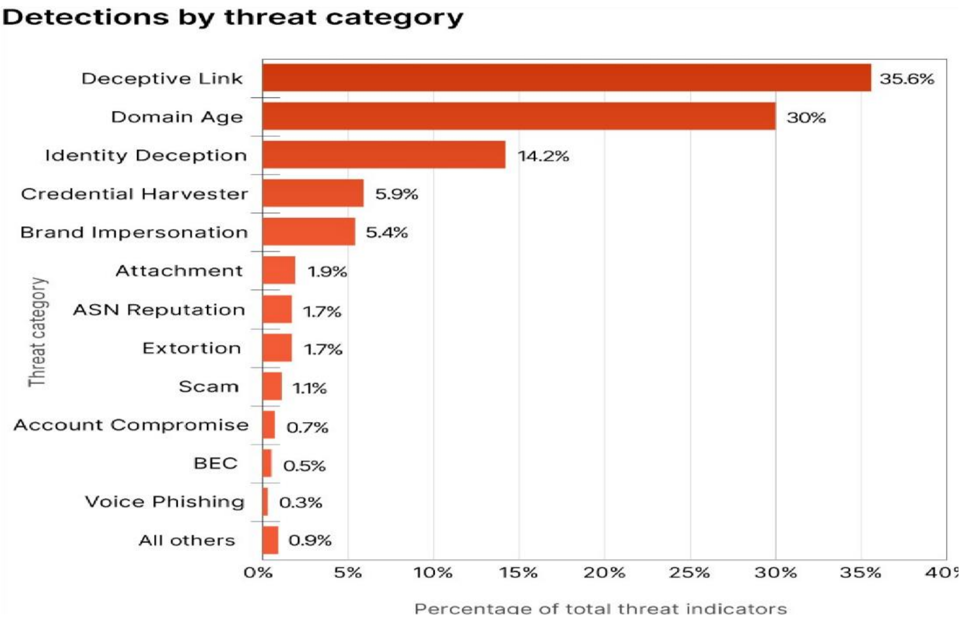
We have specifically detailed certain types of technologies and software projected to undergo significant growth in both the present and future.

“*Why are Cyber-attacks increasing?”* In this era where technology pervades every aspect of our lives, Virtual friendships on social media, engagement in online banking activities, and digital facilitation of various requirements have become commonplace. As a result, these tasks have accelerated the transition of common place criminal activities to the online world.

Presenting the emerging technologies that are used in Cybercrime.

Phishing

Phishing is a most common attack use by the attackers, it is an illicit attempt to obtain sensitive information, such as usernames, passwords, credit card numbers, bank account details, or other vital data, for the purpose of utilizing or selling the stolen information. This activity occurs when an attacker, posing as a trusted entity, deceives a victim into opening an email, instant message, or text message. Subsequently, the recipient is manipulated into clicking a malicious link, which may result in the installation of malware, system freezing as part of a ransomware attack, or the disclosure of sensitive information. Email phishing threat will be in the top position in the attack vectors, as the number of people using emails are increasing daily. The consequences of a phishing attack are severe, encompassing financial loss, identity theft, and unauthorized transactions. It is human nature to be curious about discounts and know new things. By deceiving individuals into divulging sensitive information, criminals can exploit these details for money laundering and other illicit activities. There are many types of phishing attacks-AI-Powered Phishing, Whaling, Mobile Phishing, Cloud Storage Phishing, Search Engine Phishing, Deepfake Phishing and Multi-Factor Authentication (MFA) Bypass Phishing.



Artificial Intelligence (AI) and Machine Learning (ML) and Data mining -

These are interrelated fields with distinct roles. AI involves creating computer systems capable of human-like tasks, while ML, a subset of AI, focuses on algorithms enabling computers to learn from data without explicit programming. Data mining discovers patterns in large datasets. Nowadays, AI and ML find applications in personal assistants, manufacturing, healthcare like Alexa, Siri and more, offering numerous benefits. However, drawbacks include reduced creativity, reliance on shortcuts, and potential job displacement, increase virtualization and make manpower less which has side effects on humans. AI/ML can automate, accelerate, and optimize Cyber-attacks, making them more customized and adaptable to target individuals, organizations, or groups with greater ease and frequency. In Cybersecurity, Machine Learning and data mining enhance attack detection systems, making them more intelligent. Despite their effectiveness, there's a risk of error susceptibility and delayed results, posing potential dangers. AI's growth is evident, with a projected 54% annual increase in the global AI market. Job reshaping due to AI is imminent, with over 120 million workers requiring retraining. Concerns arise about the potential displacement of 45 million American jobs by AI by 2030. Trust in AI varies globally, with 75% of respondents in a study expressing trust, differing among nations like India (67%), China (57%), and South Africa (57%) Machine learning algorithms can analyze vast amounts of data to identify specific targets for Cyber-attacks, like AI generated deepfakes, AI driven social engineering, Data manipulation and make targeted attacks.

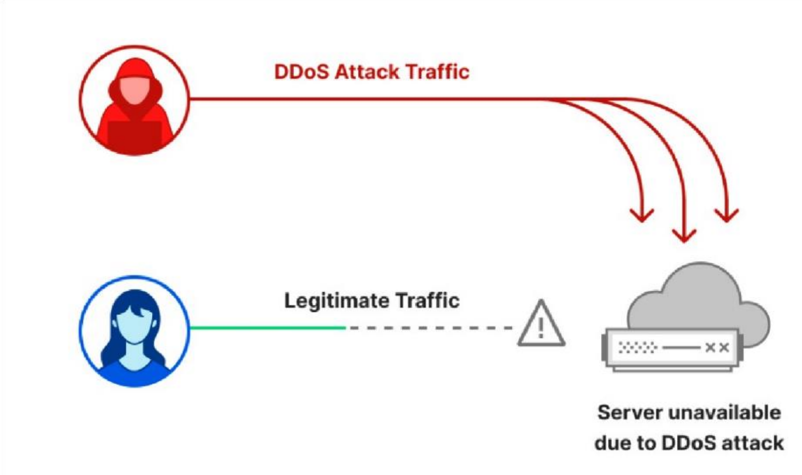
Internet of Things (IoT)- refers to the network of interconnected devices that communicate and exchange data with each other over the internet. These devices are daily objects with sensors, Software, and technologies. The adoption of IoT introduces vulnerabilities with both current and future negative impacts. The advancement of technology can increase dependency on it for daily tasks, which raises concerns about security and privacy, including the risk of data breaches and security threats. Moreover, the widespread integration of IoT could lead to job displacement, as automation and interconnected devices may replace certain human roles. The excessive use of IoT technology, especially by individuals, can lead to severe environmental impacts, emphasizing the need for responsible practices and addressing these concerns in the integration of IoT technologies.

Autonomous Devices and Systems - refers to machines or systems that can operate and make decisions independently without human involvement. These systems often work with artificial intelligence, machine learning, and sensors to perceive their environment and respond to it. Examples include self-driving cars, drones, smart home devices, and industrial robots. While autonomous devices have the potential to enhance efficiency and productivity, they also raise concerns about safety, ethical considerations, and the impact on employment in certain industries.

Remote Accessing - It is the ability of users to access a device from any location, with this user can manage data and use their system as they want. Works with the help of Virtual Private Networks (VPNs), Remote Desktop Services (RDS), and various remote access software tools facilitate remote access. While access control is designed to enhance security, hackers may attempt to exploit vulnerabilities or manipulate access control mechanisms to gain unauthorized access. They exploit weak passwords, attack through social engineering, by breach of credential with the help of phishing, malware etc. There are certain types of attacks, most discussed.

ATTACKS

1. *DoS and DDoS attack*- Now Denial of Service and Distributed Denial of Service attack are the most common Cyber threats due to use of internet in everyday life. The DoS attack is quite simple to carry out. It just needs one device and a few basic, readily available online tools. DDoS attacks are more sophisticated than DoS attacks, but with enough expertise, anyone can easily send enormous amounts of unwanted traffic to a particular IP address and terminate the victim's services.



Cloudfare- DDoS threat report for 2023

2. *Social Engineering*- In this category of the attack the focus is on human psychology. Without physically breaking in or hacking the system or network, a variety of human traits, including curiosity, rage, gullibility, cheerlessness, and rush, are utilized to obtain information to obtain illegal access or steal the data. A personnel member may violate security standards due to their emotional conduct and organizational expertise, every organization's security policy ought to cover security awareness.

3. *Ransomware*- A ransomware attack aims to install malicious software on a target's computer or network, often using phishing emails or deceiving the target into visiting malicious websites. The malware encrypts data or prevents authorized access, prompting a warning message in the form of bitcoin, outlining payment procedures and the decryption key.

1. **Threats-** There are many possible ways in which the threats, risks and vulnerabilities may occur

1. Trojon horse
2. Roolkit
3. Worms
4. Brute force
5. Darknet
6. logic bombs
7. Terrorist attacks
8. Vandalism
9. Embezzlement
10. Theft and strikes.

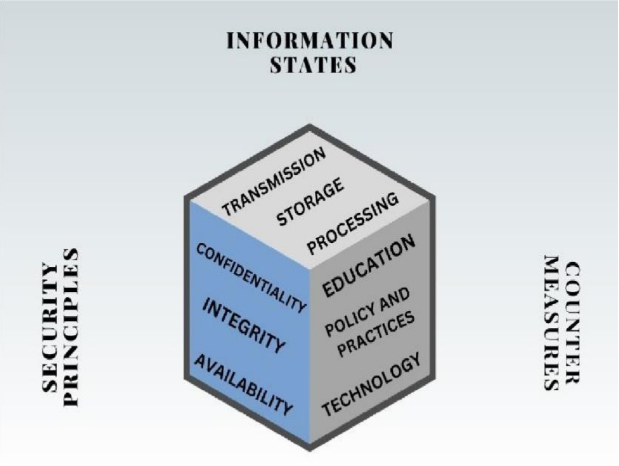
8. Technology Infrastructure

This section covers the technological aspects of Cyberspace of Cyberspace and the fundamentals of security. It discusses the basic principles of possible Cybersecurity foundation and solutions.

8.1 Cybersecurity

In Cyber criminology the central focus is on Cybersecurity, so Cybersecurity is essential for maintaining and developing technology infrastructure against Cyber-attacks and unauthorized access.

The State of Cybersecurity report highlights an increasing demand for technical skills, notably in areas such as identity and access management (49%), cloud computing (48%), data protection (44%), incident response (44%), and DevSecOps (36%). In addition to these technical competencies, there is a growing emphasis on soft skills. Communication leads the list at 55%, followed by critical thinking (54%), problem-solving (49%), teamwork (45%), and attention to detail (36%). There is a study initiated by John McCumber, in which he addresses three dimensions of Cybersecurity which are the main principles of Cybersecurity, on that security works.



Counter measures- Countermeasures refer to actions or strategies implemented within the realms of policies, practices, technologies, and user behaviors to mitigate security risks or threats.

Policy and practice -Developing and enforcing security policies and procedures is a critical aspect of maintaining a secure and resilient information technology environment. This involves creating a set of guidelines and protocols that outline how the organization manages and protects its information assets, systems, and networks. Security policies typically cover areas such as data protection, user authentication, incident response, and overall Cybersecurity practices.

Technologies- Softwares and Hardwares based solutions designed to protect information systems (examples: anti-virus, firewalls, intrusion detection systems, etc.), Together, these software and hardware-based measures constitute a comprehensive framework for protecting information systems against diverse Cyber threats. These measures collectively contribute to a robust Cybersecurity framework that addresses different aspects of security to ensure the confidentiality, integrity, and availability of data and systems.

Users- Security training plays a critical role in strengthening an organization's defenses against Cyber threats. By teaching users, the importance of security and providing them with the skills to recognize and report potential threats, companies can promote a culture of vigilance. Furthermore, managing user access is essential for maintaining a secure environment, ensuring that individuals only have access to the resources necessary for their roles. Implementing strict password policies, which include enforcing strong passwords and regular changes, adds an additional layer of protection to sensitive information, reducing the risk of unauthorized access. Together, these measures contribute to a comprehensive approach to Cybersecurity, establishing a resilient framework against potential breaches.

2- Information States

- Storage- is refers to (DAT) Data at rest where the information that is stored on a storage medium, such as in memory, on magnetic tapes, disks, or other storage devices. For security consideration it is for data at rest typically include encryption, access controls, and physical security to safeguard against unauthorized access or data breaches.
- Processing- when (DIT) Data in transit is the data actively being moved from one location to Another, typically between information systems or over a network and during data transmission include encryption, secure communication protocols, and ensuring the integrity of the data to prevent interception or tampering.
- Transmission- is the Processing which is the act of applying operations to data to accomplish goals, including calculation, analysis, or transformation. Ensuring the data's confidentiality and integrity is part of data processing security. Monitoring and access controls are put in place to stop malicious or illegal activity when manipulating data.

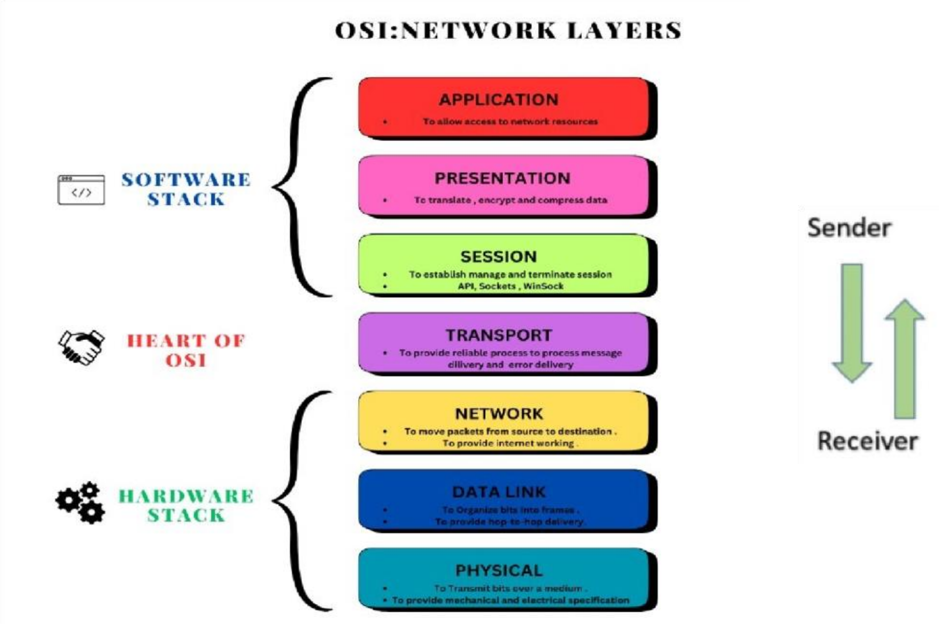
3. **Security principles**- CIA triad and Implementing access control policies, another measure to enhance security is access control policies, which determine the individuals permitted to access specific resources or information within an organization's network or system. By enforcing rigorous access controls, organizations can restrict unauthorized access, thereby reducing the risk of data breaches or other security incidents. This process includes assigning appropriate access levels to users, implementing authentication mechanisms like passwords or biometrics, and regularly reviewing and updating access permissions to align with organizational changes.

8.2 Network security

Network security encompasses the set of policies, processes, and practices implemented to prevent, detect, and monitor unauthorized access, misuse, modification, or denial of a computer network and its accessible resources. Network administration is responsible for granting access to data within a network, typically managed by the network administrator. Users can access information and programs by selecting or assigning an ID or password. This process is applicable to both public and private computer networks, facilitating transactions and communications among businesses, government agencies, and individuals. Its primary function is to safeguard the network and ensure the security of ongoing operations. A common method for strengthening network resources is assigning a unique name and password.

It includes firewalls, network access control systems, VPNs (Virtual Private Network), network segmentation, antimalware software, anti-virus, access control, application security, and cloud security. These systems are based on network protocols, which govern data exchange and authentication. Examples include SSL and TLS for secure web communication, which establish secure communication channels through encryption, authentication, and integrity checks to protect sensitive data during transmission.

OSI Model Layers- The OSI model is a conceptual framework that regulates the functions of a telecommunication process or computing system into seven layers, from the bottom (physical layer) to the top (application layer), and vice versa:


OSI:NETWORK LAYERS
SOFTWARE STACK
HEART OF OSI
HARDWARE STACK
APPLICATION
To allow access to network resources
PRESENTATION
To translate , encrypt and compress data
SESSION
To establish manage and terminate session
API, Sockets , WinSock
TRANSPORT
To provide reliable process to process message dilivery and error delivery
NETWORK
To move packets from source to destination .
To provide internet working .
DATA LINK
To Organize bits into frames .
To provide hop-to-hop delivery.
PHYSICAL
To Transmit bits over a medium .
To provide mechanical and electrical specification
Sender
Receiver

8.3 Principles of Information security

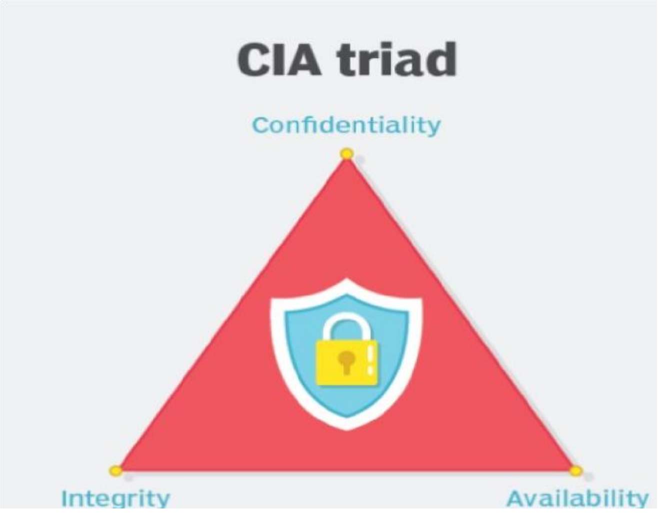
Information security is the protection of sensitive information of an organization. It is also known as Info-sec. commonly referred to as Data security, its primary objectives are safeguarding information and data such as customer account details, financial data, intellectual property, government critical information, and confidential information from unauthorized access, disclosure, alteration, and destruction. It includes policies, tools, frameworks, and processes. Information security has three fundamental principles, the CIA Triad: Confidential, Integrity, and Availability, which signifies the role of accountability and authenticity of information and data. For clarification,

- Integrity refers to the accuracy, quality and consistency of information that remains unchanged by any third party. It ensures the accuracy and reliability of data and information, which means that data should not be altered or transformed by any unauthorized parties. Techniques such as hashing, checksums, and digital signatures are used to verify data integrity. It also involves protecting data from accidental alterations.

- Confidentiality of information ensures that only those with sufficient privileges may access certain information, i.e., only authorized individuals or systems should be able to access and view sensitive or confidential data. Through encryption, access controls, and data classification are used to maintain confidentiality.
- Availability is making information available to the user, the authorized person, or the organization that needs to access it without interference and obstructions in the given format. It can be available through redundancy, backup systems, and disaster recovery plans must maintain availability.

Now, identification and accountability are also the key concepts of information security were identification stands for your information possesses the characteristic of identification when they can recognize individual user and accountability stands for his control is implemented to establish accountability for actions and helps in monitoring and tracking activities to identify any potential security breaches or issues. Other measures are Risk management, Security policies, Security awareness and training, technologies, Contingency planning, and Compliance.

Information Security is a continuously evolving field due to ever changing threats and technologies, it requires proactive monitoring of systems and organizations by Cybersecurity professionals and CISO's.



8.4 Frameworks, Standards, and Policies.

Cybersecurity frameworks and standards are essential sets of recommended practices, directives, and methodologies designed to assist organizations in complying with legal requirements and fortifying their defenses against Cyberattacks. These frameworks, formulated by experts, are applicable across diverse sectors, industries, and organizational sizes. Examples of significant Cybersecurity frameworks include NIST (National Institute of Standards and Technology), COBIT (Control Objectives for Information and Related Technologies), CIS (Critical security controls) controls, and GDPR (General Directive Protection Regulation). These frameworks, grounded in industry best practices and standards, serve as comprehensive guides for enhancing Cybersecurity posture. One prominent example is ISO 27001, also known as ISO/IEC 27001:2022, an information security standard established by the International Organization for Standardization (ISO). ISO 27001 provides a robust framework and guidelines for establishing, implementing, and managing an information security management system (ISMS), ensuring a systematic approach to safeguarding information.

Policy forms the fundamental cornerstone of a robust information security program. A policy is a plan or course of action that influences and determines decisions. Policies hold significant value as reference materials for internal audits and in resolving legal disputes related to management's responsibility. Policy documents serve as a clear expression of management's intentions.

1. ***Enterprise Information security policy (EISP)*** **–** EISP is a document that outlines the security policy of an organization or company.
2. ***Issue Specific security policy (ISSP)*** **–** ISSP is a type of security policy that addresses specific areas of organizations, provides detailed guidelines to direct the organization in secure use of technology systems, and begins with introduction to fundamental technological philosophy of the organization such as electronic mail use of the Internet Specific minimum configurations of computers to defend against worms and viruses.
3. ***System Specific security policy (SysSSP)*** **–** SysSSP is provides information about the actions that are permitted and not permitted on a specific system. It also details the procedures to configure and maintain that system.

8.5 Result

The above elaboration focuses on Cybercrime, data analysis, emerging technologies, and their effects on individuals, while also detailing the technological infrastructure for Cyber and information security. Technologies can produce more power when used in a useful way and in appropriate contexts, this section delves into the implemented solutions within the Cybersecurity domain. Here are some, Technical and non-technical solutions that can be implemented to secure the data and privacy of an individual.

Technical

Firewalls, Malware scanners and Antivirus are similar technologies, The primary function of antivirus software is to safeguard systems from malicious software by detecting and removing viruses and other harmful programs. They work to detect malware and vulnerability from unauthorized access or from any websites which have cookies and malware.

Blockchain Technology- Blockchain technology is a distributed and immutable ledger that streamlines the recording of transactions and the tracking of assets within a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Encryption- is used to protect data from being stolen, changed, or compromised, Utilize end-to-end encryption for sensitive data both in transit and at rest. Ensure that communication channels, databases, and storage systems employ strong encryption algorithms.

Access control- Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control employs policies to authenticate users and verify their claimed identities while ensuring the provision of appropriate access levels. The implementation of access control stands as a vital element in web application security, guaranteeing that only authorized users obtain the correct level of access to specific resources. This process plays a pivotal role in assisting organizations in averting data breaches and combating various attack vectors, including buffer overflow attacks, Krack attacks, on path attacks, or phishing attacks./@

Nontechnical

These solutions refer to without using any technology; they only require human awareness, which includes implementing strong passwords, using trusted sources rather than pirated ones, and regular monitoring of network traffic. Security Information and Event Management (SIEM) Systems: The fundamental function is to collect and analyze log data to detect responses to security incidents through the monitoring and analysis of system events. Additionally, organizations should consider conducting regular security assessments and staying informed about the latest developments in Cybersecurity to continuously improve their defensive measures.

9. CONCLUSION and RECOMMENDATIONS

This comprehensive review paper summarizes Cybersecurity problems and solutions based on recent technological advances. The discourse has provided a comprehensive examination of the intersection between Cybercrime, data analysis, emerging technologies, and their profound impact on individuals. It has also elucidated the technological infrastructure crucial for ensuring Cyber and information security. As technology wielded judiciously can amplify power, this section emphasized implemented solutions within the Cybersecurity domain. Safeguarding against the evolving aspects of Cyber threats requires a varied approach that incorporates advanced technological measures. The implementation of next-generation firewalls, increased antivirus solutions leveraging behavioral analysis, robust access control policies, thorough encryption protocols for data protection, and the integration of multifactor authentication collectively form a resilient defense mechanism. As a result of these proactive measures, organizations can significantly enhance their Cybersecurity posture, effectively mitigating risks associated with emerging technologies in Cybercrime. The outcome is a fortified security infrastructure that not only addresses current challenges but also anticipates and adapts to future threats. To further bolster Cybersecurity resilience, it is crucial for organizations to regularly update these technical safeguards, conduct comprehensive security assessments, and stay informed of the latest developments in Cybersecurity. By adhering to these recommendations, organizations can foster a secure environment that safeguards sensitive information and maintains the integrity of their digital operations.

ACHNOWLEDGMENT:

Author's extended gratitudes to all those authors who contributed to the successful completion of this Article. We appreciate the insights and collaboration from colleagues and the invaluable resources provided by various institutions and websites.

11. REFERENCES

Research Paper Review-

1. Dr. Yusuf Perwej et al (2021) International Journal of Scientific Research and Management (IJSRM).
2. Benoit Dupont (2021), Enhancing relationships between criminology and Cybersecurity, Centre international de criminologie comparee, Universite de Montreal, Montreal (Quebec), Canada
3. Ömer Aslan at el (March 2023) A Comprehensive Review of Cybersecurity Vulnerabilities, Threats, Attacks, and Solutions, MDPI (Multidisciplinary Digital Publishing Institute) Switzerland.

4. Jacopo Bellasio et.al (2020) The Future of Cybercrime in Light of Technology Developments- RAND Corporation, Santa Monica, Calif., and Cambridge, UK.

Online Resources

1. Cybersecurity and Criminological aspects; https://en.wikipedia.rg, https://www.britannica.com,
2. Cybercrminology- https://www.Cybercrimejournal.com, https://criminology.fsu.edu.
3. Cyberspace Terms and Definations- www.oxfordbiblographies.com, www.geegksforgeeks..org.com
4. Cyberattacks report; https://www.getastra.com/blog, https://www.statista.com.
5. Covid 19 era attacks- https://www.fbi.gov/investigate/Cyber.
6. NCRB report of Cybercrime- https://pib.gov.in/PressReleseDetailm.aspx.
7. Cyber-attack: India sees sharp increase in Cyberattacks in Q1 2023: report - The Economic Times
8. (indiatimes.com https://m.economictimes.com/tech/technology/sharp-increase-in-Cyberattacks-in-india-in-q1
9. Detection threat report: https://blog.cloudflare.com/2023-phishing-report and https://www.haekka.com.
10. Cloudfare DDoS Attack- DDoS threat report for 2023 Q4 (cloudflare.com).
11. AI and ML and Data mining reports and impacts: statista.com, https://www.simplilearn.com,
12. Autonomous Devices- https://www.simplilearn.com,
13. Remote accessing- https://seo.ai and https://www.forbes.com.
14. Use of IOT- https://www.ibm.com/topics/internet-of-things
15. Study of ISO/IEC 27001, Information security standard in context of SMEs and frameworks and standards
16. 2019MCLIS20_Dissretation.pdf.
17. Cybersecurity, https://www.isaca.org.
18. John Maccumber Cube: wikipedia.com and https://www.researchgate.net/figure/The-Original-McCumber-
19. Model_fig1_235470635.
20. Solutions technologies: https://www.fortinet.com and https://www.ibm.com/topics/Cybersecurity.
21. Future of cybercrime light of technology developments- https://www.rand.org