GE-International Journal of Engineering Research
ISSN(O): 2321-1717, ISSN(P): 2394-420X
Vol. 12, Issue 9, September 2024 Impact Factor- 8.261

Website-www.aarf.asia, editoraarf@gmail.com

# METHODS OF ATTACKS ON CYBERSECURITY AND ROLE OF AI DETECTION

**Manoj Kumar[1] Dr. Kuldeep Kumar[2]**

1. **Research Scholar, Shri Khusal Das University Hanumangarh**

2. **Research Supervisor, Shri Khusal Das University Hanumangarh**

***ABSTRACT***

*AI detection mechanisms, as mentioned in the title, signifies a crucial step forward in the ongoing battle against cyber threats. These AI-driven tools not only provide a more robust defense against evolving cyber-attacks but also contribute to the continuous evolution of cyber security strategies. Nevertheless, it is essential to acknowledge that AI detection is not a panacea; it requires constant refinement and adaptation to stay ahead of the ever-evolving tactics employed by cyber adversaries. The concepts of cyber security as clearly as possible and have provided numerous cyber threats and attacks to understand those concepts.*

***Keywords:*** *Methods , Attacks , Cyber security, Role , AI , Detection*

## INTRODUCTION

In the contemporary landscape, the pervasive integration of digital technologies into every facet of human existence has ushered in an era of unprecedented connectivity and efficiency. This phenomenon, commonly referred to as Digital Transformation (DT), encompasses the infusion of digital capabilities into traditional processes, thereby revolutionizing the way businesses, governments, and individuals operate. While DT promises remarkable advancements in productivity, innovation, and convenience, it concurrently exposes an intricate web of vulnerabilities, placing critical systems and sensitive information at risk. Among the most pressing concerns within this paradigm is the escalating threat landscape of cyber security. As organizations race to embrace the benefits of digitalization, the attack surface for cyber threats expands exponentially. The interconnectivity of devices, the proliferation of cloud computing, and the rise of Internet of Things (IoT) have created a complex ecosystem where security breaches can have far-reaching consequences. The paradigm shift towards remote work and the decentralization of data storage further amplify the challenges faced by cybersecurity professionals. In this context, it becomes imperative to explore and understand the

multifaceted challenges that emerge as a result of the symbiotic relationship between digital transformation and cyber security. This research paper seeks to delve into the intricate nuances of cyber security challenges in the era of digital transformation. By synthesizing current literature, empirical data, and case studies, the study aims to provide a comprehensive overview of the evolving threat landscape. From sophisticated cyber-attacks targeting critical infrastructures to the vulnerabilities introduced by emerging technologies, the research will dissect the various dimensions of cyber security concerns in the digital age.

The NISTIR 7298 report (Glossary of Key Information Security Terms, July 2019) defines the cyber security concept as measures used to protect confidentiality, integrity, and availability of system, and data (such as software, hardware, network), and information being processed, stored, and communicated. This definition represents the concepts of confidentiality, integrity, and availability that build what is merely referred to as the CIA triad. These three concepts are at the heart of cybersecurity and include security goals for information and computer systems. The FISMA (Standards for Security, Categorization of Federal Information and Information Systems, February 2004) defines three security goals for information and computer systems:

- **Confidentiality:** Considering permissible limits on access and disclosure of information, including tools to protect sensitive personal information and proprietary information.

- **Integrity:** Protection against correction or destruction of false information, including ensuring non-repudiation and accuracy of information.

- **Availability:** Ensuring timely and reliable access of authorized users to resources when needed

Depending on an organization's security objectives and their regulatory requirements, one of these three concepts (confidentiality, integrity, and availability) might take precedence over another. For example, confidentiality is critical for certain government agencies; integrity is vital for financial sector; and availability is important in both the ecommerce and the healthcare sector (Dalziel, 2014). An organization could decide how to use these three concepts given their specific requirements, balanced with their goals to develop a seamless and safe user experience. An organisation that requires high confidentiality and integrity might sacrifice lightning-speed performance that other organisations might value more highly.

**Role of AI Detection in Cyber security**

To counter the growing sophistication of cyber threats, organizations are increasingly turning to artificial intelligence (AI) for cyber security. AI detection systems leverage machine learning algorithms to analyze vast amounts of data, identify patterns, and detect anomalies indicative of potential security incidents. The literature reveals that AI-based approaches offer real-time threat detection, proactive risk mitigation, and enhanced incident response capabilities.

Furthermore, AI-driven threat intelligence enables organizations to stay ahead of evolving threats by continuously learning and adapting to new attack vectors. Researchers highlight the potential of AI in automating routine cyber security tasks, allowing human experts to focus on more complex and strategic aspects of cyber security management

**Methods Of Attacks And Avoidance**

The most popular weapon in cyber attacks is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism' .The attacks or methods on the computer infrastructure can be classified into three different categories.

**1. Physical Attack.** The computer infrastructure is damaged by using conventional methods like bombs, fire etc.

**2. Syntactic Attack.** The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictab le. Computer viruses and Trojans are used in this type of attack.

**3. Semantic Attack.** This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user's knowledge in order to induce errors.

**Types of Risks** The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

**Viruses -** This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

**Worms -** Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.

**Trojan horses -** A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your

computer may actually be sending confidential information to a remote intruder.

**Hacker, attacker, or intruder -** people who exploit weaknesses in software and computer systems for their own gain. Though they do it for curiosity, their actions are typically in violation of the intended use of the systems. The results can range from creating a virus with no intentionally negative impact to stealing or altering information.

**Malicious code -** This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.

**E-Mail Related Crime-** Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.

**Denial of Service** -These attacks are aimed at denying authorized persons access to a computer or computer network.

**Cryptology-Terrorists** have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

**OBJECTIVES OF THE STUDY**

1. To study on Cyber Security Initiatives In India
2. To study on Role of AI Detection in Cybersecurity

**Cyber Security Initiatives In India**

ISO 27001 (ISO27001) is the international Cyber security Standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System. Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce. IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere. According to Ministry of Electronic and Information Technology, Government of India: Cyber Laws yields legal recognition to electronic documents and a structure to support efiling and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

**A) Importance of Cyber Law:**

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

**B) Area of Cyber Law**

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

**a) Fraud**

Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

**b) Copyright**

The internet has made copyright violations easier. In early days of online communication, a copyright violation was too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

**c) Defamation:**

Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

**d) Harassment and Stalking**

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws.

**Cybersecurity Landscape in the Era of Digital Transformation: Identifying Key Threats and Vulnerabilities**

The critical analysis of the evolving cybersecurity landscape revealed a myriad of challenges faced by organizations amidst the ongoing digital transformation. Rapid technological advancements have given rise to new threats and vulnerabilities, ranging from sophisticated malware to targeted attacks on interconnected systems. The review underscores the importance of understanding these evolving threats to develop proactive and adaptive cybersecurity strategies.

**Impact of Digital Transformation on Traditional Cybersecurity Measures: Balancing Opportunities and Risks**

The assessment of the impact of digital transformation on traditional cybersecurity measures emphasized the dual nature of emerging technologies. While the integration of IoT, cloud computing, and AI presents unprecedented opportunities for efficiency and innovation, it also introduces new avenues for cyber risks. The discussion delves into the delicate balance required to harness the benefits of these technologies while mitigating the associated cybersecurity risks effectively.

**Role of Artificial Intelligence in Cybersecurity Defenses: Detection, Mitigation, and Limitations**

The evaluation of artificial intelligence's role in enhancing cybersecurity defenses revealed its promising potential in detecting and mitigating cyber threats. AI algorithms demonstrated effectiveness in real-time threat detection, incident response, and anomaly detection. However, the discussion also highlights the limitations of AI, such as susceptibility to adversarial attacks and the need for continuous improvement in adapting to evolving cyber threats.

**Regulatory and Compliance Frameworks in Cybersecurity: Addressing Digital Transformation Challenges**

The examination of regulatory and compliance frameworks governing cybersecurity practices illuminated the challenges faced by these frameworks in keeping pace with the dynamic landscape of digital transformation. The review calls attention to the need for adaptive and robust regulatory measures to ensure that policies align with the evolving nature of cyber threats and technological advancements. Recommendations are proposed to enhance existing frameworks for better resilience against emerging challenges.

**Strategies and Best Practices for Cybersecurity in Various Sectors during Digital Transformation**

The investigation into strategies and best practices employed by organizations in different sectors underscored the diversity of approaches to address cybersecurity challenges during digital transformation. Successful approaches were identified, emphasizing the importance of a holistic cybersecurity strategy that combines technology, employee training, and collaboration with stakeholders. The discussion also identifies areas that require further research and development, such as the need for sector-specific cybersecurity frameworks.

## CONCLUSION

The advent of AI detection mechanisms, as mentioned in the title, signifies a crucial step forward in the ongoing battle against cyber threats. These AI-driven tools not only provide a more robust defense against evolving cyber-attacks but also contribute to the continuous evolution of cybersecurity strategies. Nevertheless, it is essential to acknowledge that AI detection is not a panacea; it requires constant refinement and adaptation to stay ahead of the ever-evolving tactics employed by cyber adversaries. The concepts of cybersecurity as clearly as possible and have provided numerous cyber threats and attacks to understand those concepts. However, many organisations will wish to identify and manage those threats and attacks and analyse risks. This chapter also provides some frameworks and guidelines and describes security protocols available in that regard. Finally, two concepts: security awareness program and security training program can facilitate managers and users within an organisation to protect their valuable and sensitive information/ data. Security awareness program refers to inform and focus a users' attention on issues related to security within the organization. Such programs includes security basics and literacy factors, given the widespread utilisation of information systems in organizations. Therefore, users are aware of their responsibilities for securing data and the restrictions on their activities in the interests of security, and are motivated to act accordingly.

## REFERENCES


[1]. Rao, Sushma & Nair, Sandeep & Joseph, Moly. (2018). Cybersecurity: What Everyone needs to know Cybersecurity: What Everyone needs to know.

[2]. Lošonczi, Peter. (2018). Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population. Security Dimensions. 26. 173-186. 10.5604/01.3001.0012.7249.

[3]. Dummanaboyina, Chakravarthy. (2020). CYBER SECURITY AND ITS IMPORTANCE.

[4]. Sheth, Mrs & Bhosale, Sachin & Kurupkar, Mr & Prof, Asst. (2021). Research Paper on Cyber Security. 2021.

[5]. Kalakuntla, Rohit & Vanamala, Anvesh & Kolipyaka, Ranjith. (2019). Cyber Security. Holistica. 10. 115-128. 10.2478/hjbpa-2019-0020.

[6]. Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.

[7]. Mindcore, M. (2018, September 5). 5 types of cybersecurity. Retrieved February 5, 2021, from https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

[8]. Al Amro, S. (2020). How safe is governmental infrastructure: A Cyber Extortion and Increasing Ransomware Attacks Perspective. International Journal of Computer Science and Information Security (IJCSIS), 18(6).

[9]. Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. (2020). Toward a Sustainable Cybersecurity Ecosystem. Computers, 9(3), 74. https://doi.org/10.3390/computers9030074

[10]. Walstrom, M. (2016). "India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges." Seattle: Henry M. Jackson School of International Studies.

[11]. Aiyengar, S. R. R. (2020). National Strategy for Cyberspace Security. New Delhi: KW Publisher

[12]. Athavale, D. (2018). "Cyberattacks on the Rise in India." The Times of India, Pune, March 10.

[13]. Bamrara, A., G. Singh and M. Bhatt (2019). "Cyber Attacks and Defence Strategies in India: An Empirical Assessment of the Banking Sector." International Journal of Cyber Criminology, 7 (1): 49–61.

[14]. Cavelty, M. D. (2022). "The Militarisation of Cyber Security as a Source of Global Tension." In Mockli, Daniel, Wenger, and Andreas, eds. Strategic Trends Analysis. Zurich: Center for Security Studies

[15]. Dilipraj, E. (2019). "India's Cyber Security 2013: A Review." Centre for Air Power Studies, 97 (14): 1–4