A Review on Cyber Security Challenges and Threats in modern world

Mahima[1*]

[1]Research Scholar (MTech Student),
Dept. of Computer Science and Engineering, UIET, Maharshi Dayanand University, Rohtak, India,

DOI: 10.64823/ijter.2605004

***Abstract*:** Theoretical frameworks and empirical findings consistently underscore the prominence of cybersecurity awareness as a central theme in contemporary cybersecurity research. This review paper aims to gain knowledge about the term 'cybersecurity' and the need to analyze and identify various kinds of threats that a person or organization may face in this information era, because as connectivity increases, the devices can interact and share information, and this could lead to a rise in cybersecurity risk.

This paper covers various threats, including malware, ransomware, phishing, data breaches, and physical manipulation. These threats carry potential consequences such as financial loss, psychosocial impacts, erosion of trust, and unauthorized disclosure of sensitive data.

"This discussion examines AI-enabled defence strategies and procedural frameworks that contribute to strengthening cybersecurity awareness and protection." This paper is based on data collected from government agencies.

This paper defines cybersecurity and discusses various cybersecurity threats like phishing, data breaches, ransomware, denial of service, and advanced persistent threats. The primary goal is to lower expenses brought on by cybersecurity risks.

***Index Terms*:** Cybersecurity; Ransomware; IoT attacks; Phishing; Data breaches; Protective measures; User awareness

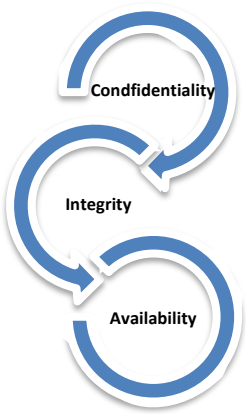
I. INTRODUCTION

As of October 2025, approximately 6.04 billion people worldwide were using the internet, representing 73.2% of the global population. Among them, about 5.66 billion individuals, or 68.7% of the world's population, were active on social media platforms (Ani Petrosyan, 2025).

This gradually resulted in the gathering and archiving of an enormous volume of data, including private information, in a variety of spheres of human endeavor, including business, education and healthcare. Cybersecurity refers to the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks, also known as information technology security [1]. Cisco Systems, a technology firm that specializes in networking, cloud, and security, defines cybersecurity as protecting systems, networks, and programs from digital threats [2]. Simply because the information contained in computer systems is so vital, computers are among the most appealing systems for unauthorized individuals to take control of [3].

There are several definitions of cyberattacks and cybercrime in the international literature, but they all attempt to comprise data confidentiality, integrity, and availability. [4].

Confidentiality: Confidentiality is defined in ISO/IEC-17799 as "ensuring that information is accessible only to those authorized to have access." The confidentiality is intended to make sure that the data is only available to those who are entitled to it for reading, listening, recording, or physical removal. [5]. The basic premise of integrity is to prevent certain aspects or assets of information from being improperly altered [6]. When we talk about availability, we imply that data should always be accessible to authorized users. [7]. Information is useless if it is not available when needed. Information unavailability is just as detrimental to a business as a loss of integrity or confidentiality.



Problem Statement:
Although technology provides amazing upside in facilitating our daily tasks, it is still inconceivable to lose sight of the obstacles that come with it. The cybersecurity threats and their severity continue to escalate constantly, which is one of the primary hurdles.

II. METHODOLOGY:

Various online databases were exhaustively searched to compile this literature review. Furthermore, these comprised Google Scholar, ACM Digital Library, ResearchGate, Scopus, SpringerLink, Arxiv, ScienceDirect, and IEEE Xplore. Relevant studies and publications were identified by using terms such as "cybersecurity" and "threats."

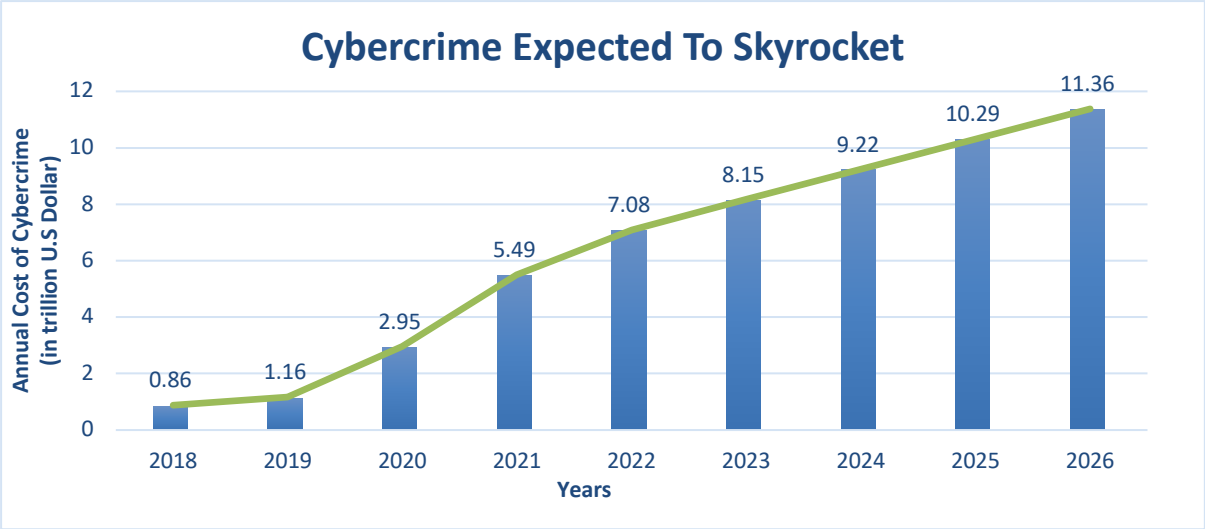
III. EVOLUTION OF CYBER ATTACKS

The world has seen a cybersecurity evolution over the past few decades. Several decades prior, cyber risks consisted mainly of easily detectable viruses. Nowadays, we face sophisticated threats. The evolution of cyberattacks can be traced through multiple stages. [8].

1. **The First Stage: Conventional Attacks:**
   Viruses and Worms: In the early years (1970s-1990s), cyberattacks on computers were straightforward and frequently targeted viruses and worms that propagated via email and physical media such as floppy disks. More than half of these early risks are localised, and there were few security safeguards [9]
   Example: Michelangelo Virus in 1990, The Morris Worm in 1988.
2. **The Second Stage: Organized Attacks:**
   Attackers and hackers adopt structured tactics to quickly penetrate systems [10].
   Growing Internet and Web-Based Threats: This generation of attacks helped to create early IDS systems, which quickly evolved into Intrusion Prevention Systems by adding corrective functionality. Tens of millions of Windows computers are being infected by a worm called LOVEYOU (2000) [11].
3. **The Third Stage: Complex and Funded Attacks:**
   Attackers now frequently encrypt files and demand a ransom in return. Some of the well-known examples of attacks that resulted in large losses worldwide were WannaCry and Petya [8].
4. **The Fourth Stage: Cross-Border Attacks:**
   Cyberattacks on supply chains target businesses by taking advantage of weaknesses in supply chains, as is witnessed with the SolarWinds security breach that impacted several companies and authorities globally.
5. **The Fifth Stage: Smart and Sophisticated Attacks:**
   Leaked powerful weapons-grade hacking tools enable attackers to move quickly and infect a significant number of businesses. For instance, 614 Gigabytes of data on weapons, sensors, and communication systems were purportedly taken from US Navy contractors by Chinese government hackers [12].

IV. The Price of Cyber Attacks:

US National Security Agency (NSA) Director General Keith Alexander referred to cyber espionage as "the greatest transfer of wealth in history." [13].



Cybercrime is thought to cost up to 10.29 trillion US dollars worldwide. There is an analysis that illustrates how costs continue to rise and the pattern they are following. The predicted costs for 2026 are additionally built on past statistics. Statista Market Insights assisted in this graph.

V. Types of Cybersecurity Threats

1. **Phishing:**

   Last Drager (2014) performed an in-depth examination of the definition of phishing and discovered a widely accepted term: 'Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target.'

   Phishing technologies are made up of three aspects [14]

   a. Medium of Phishing: It is the primary mechanism for delivering phishing assaults to the targeted individuals. It includes Internet accessibility and SMS.

   b. Vector to transmit the attack: The vector of communication adopted by the phishers depends on the medium that serves as the vehicle for initiating phishing attacks. Smishing is the phishing vector by SMS [14].

   c. Technical Approaches: These are the approaches used in furtherance of social engineering phishing in order to boost the efficacy of phishing, e.g., cross-site scripting.

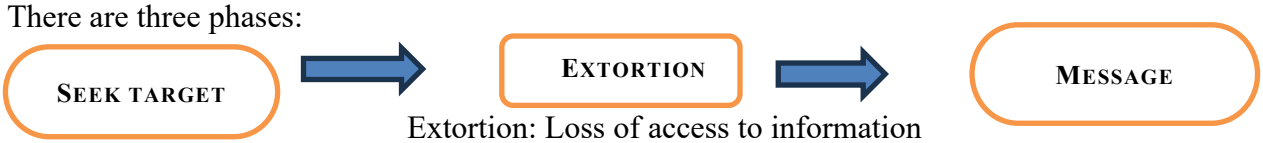
2. **Ransomware:**

   The terms "ransom" and "malware" together form the building blocks of ransomware.

   One general definition: "A type of malware referred to as ransomware requests money in return for a feature that has been stolen." [15].

   Criminals host websites that provide Ransomware-as-a-Service (RAAS). Additionally, there are free online development kits like TorLocker [16] and TOX that can be used to generate ransomware Trojans and launch attacks.

   There are three phases:

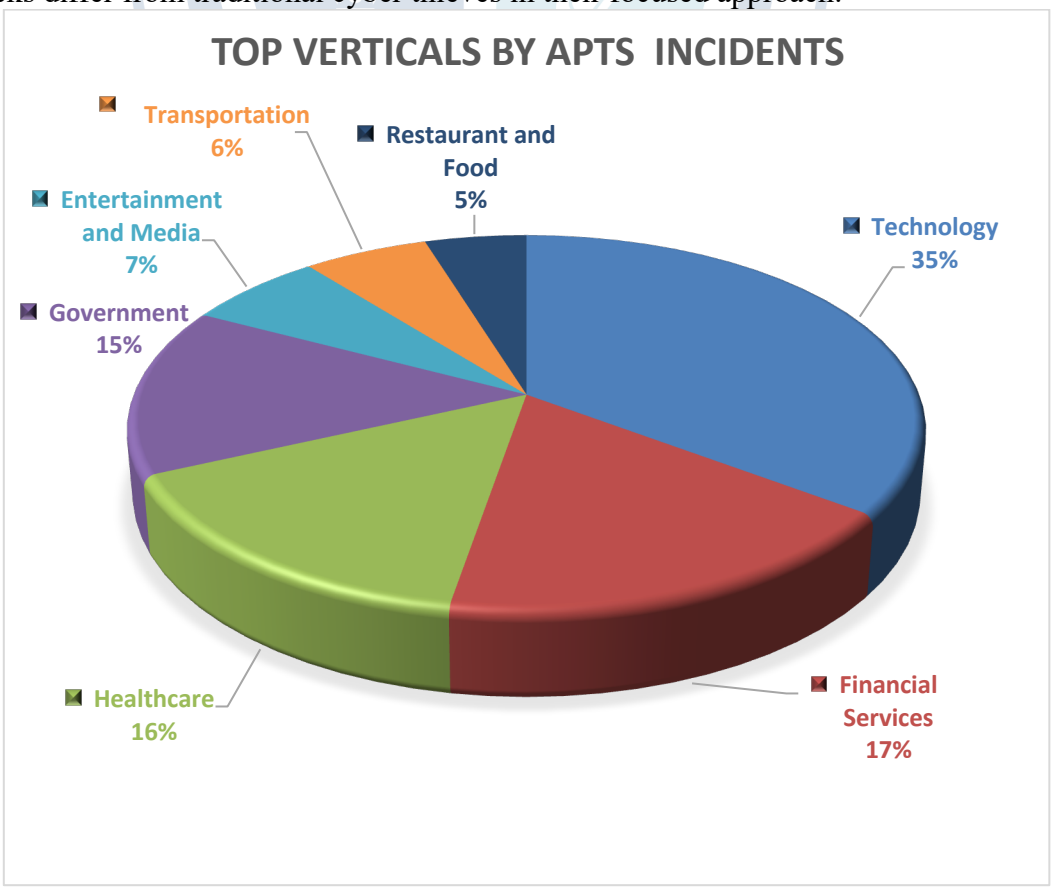


Extortion: Loss of access to information

3. **Denial of Service (DoS):**
   The main objective of a DDoS attack is to impose a disruption on the target users, who are typically referred to as "victims." In general, a DDoS attack aims to hinder access of legitimate users to a target system or services by overwhelming the resources [17].
   SYN Flood Attack and UDP DDoS Attack are the most popular DDoS attacks at the moment. In both, an extensive number of packets are sent to particular ports on the intended IP address(es). We can defend these attacks by using Cloudflare Magic Transit and Zero Trust Network Access (ZTNA).
4. **Data Breaches:**
   The deliberate or unintentional disclosure of confidential details to illicit parties is known as a data breach [18]. Internal and external information breaches, whether deliberate (such as data theft by hackers) or unintentional (such as the accidental disclosure of sensitive data), can result in data leakage. To stop data breaches, there are numerous methods commonly known as Data Leak Prevention and Detection Technique (DLP). DLP technology enforces the rules governing the movement of data into and out of the organization's electronic network, including notification, response actions, and audit trails [19]. Some of the DLP techniques are regular expressions [20] and fingerprinting [21] [22].
5. **Advanced Persistent Threats (APTs):**
   APTs are sophisticated, long-term cyberattacks, frequently carried out by powerful nations or financially strong groups. Detecting and combating APTs poses a big problem because they use complex strategies to avoid typical security systems [23]

   The components of the terminology defined by the United States Air Force (USAF) are:
   a. Advanced: the enemy is familiar with the tool and technique of intrusion and can design bespoke exploits [24].
   b. Persistent: the opponent fulfils a purpose and receives commands.
   c. Threat: the enemy has been supervised and supported.

   Approaches used for APTs Detection: dynamic analysis [25] and context-base [26].
APT attacks differ from traditional cyber thieves in their focused approach.



VI. LITERATURE REVIEW:

In [27] Jamal proposes an innovative analytical method for identifying cyberattacks. He predominantly employs three tactics for that. Misuse: Misuse detection identifies hackers exploiting known attack patterns and system weaknesses. It is expected of security administrators to recognize them. Artificial Immune System: The presence of foreign microbes in the human body may be identified and diagnosed by the biological immune system (BIS). He employed BIS-inspired co-stimulation to cut down on false positives and boost network misbehaviour detection's energy efficiency. Anomaly: Cyberattacks are assumed to cause divergences from common conduct in anomaly detection. It can be a dynamic or static process. Static detection examines the integrity of system components that remain unaltered, such as OS files or boot data, while dynamic detection evaluates data that undergoes modifications, like audit records. Majorly dynamic focus on ongoing operations to identify suspicious patterns and static search for variations in fixed system elements.

In [28] Nikolaos proposed a NEON framework. NEON is a highly automated, multiple-stage APT detection tool that employs game theory, honeypots, adversarial machine learning defence, and information gathering to recognize complex assaults and locate their origin. For the implementation of the collector and analyser, he used Content Crawler, Content Analysis, and Content Linking, which gather APT-related reports by automatically scouring the internet and archives. It used adversarial ML approaches to extract malware names and IPs from gathered data. In network monitoring, it collects data for each network flow, and for that, it uses Deep Packet Inspection (DPI). It sends information to NEON Incident Detection & Classification (IDC) if there is some suspicious activity. And the IDC performs prioritization, filtering, and normalization on data. Then it carries out correlation of security events to find out risk assessment, and then it generates an alarm by the NEON Attack Alert (AAlrt) component. If there are adversary indicators and mitigation is required, then the Game Theoretic Defence (GTD) component is used to suggest the best safeguards against the APT offender. To prevent future attacks, NEON DSB will develop an interactive, user-friendly visualization dashboard using data collected by NM, IDC, and GTD.

In [29] Leandros Maglaras discussed cybersecurity measures. He categorized them as legal, technical, organizational, capacity building, and dimensional. Legal Measure: The execution required regular evaluations of critical infrastructure via information security audits and regular maintenance of software and hardware that are used in critical infrastructure. Technical Measure: The deployment of defensive and detective security tools, consisting of firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and antivirus solutions. Organizational Measures: Any sort of national initiative or strategy needs to be effectively carried out, and this requires organizational measures. Organizations ought to perform security audits to evaluate their level of cybersecurity readiness. Capacity Building Measures: Encourage IT professionals from globally renowned cybersecurity programs and recurrent staff awareness and training campaigns. Cooperation measures: To enhance an organization's cyber resilience against cyber threats, cooperation measures attempt to promote collaborations between different groups of stakeholders.

In [30] Muritala Aminu discussed real-time threat intelligence. The acquisition of information prior to a cyber attacker approaching a victim system is referred to as cyber threat intelligence. To recognize and mitigate cyber threats, processing and analysing data is essential. Data is gathered from outlets such as endpoint telemetry and network logs. Platforms for real-time processing, like Apache Kafka and Apache Spark Streaming, are utilized. Then, normalization is performed on the collected data to organize various data types. This involves mapping data fields and correcting timestamps. On the normalized data, we apply statistical analysis, machine learning techniques, and pattern recognition in order to find out irregularities and indications of penetrations. And it will give a rank alert according to the impact of the threat. Threat maps provide impacted assets, which enable administrators to quickly make educated decisions. Threat intelligence sharing is essential for improving the efficiency of real-time threat intelligence to allow information sharing between firms. Various platforms, like Information Sharing and Analysis Centres (ISACs), are used.

In [10] M. Uma discussed that the main target of cyberattacks is the data or information of governmental websites and military/defence websites. Obstruction of Information: Attackers restrict access to authorized individuals from accessing critical data within a government agency during vital moments. Counter International Cyber Security Measures: Attackers increase their attack complexity so that they can defeat the measures of cybersecurity to reduce cyberattacks. Retardation of the Decision-Making Process: In defence

during any emergency, they cause a delay in decision-making by tactical deployment, which can lead to military defeats. Denial in Public Services: They block users from accessing their banking, railway, and airline services. Abatement of Confidence: Due to hacking, there is a loss in people's confidence in the security of a firm. The main motive of a cyberattack is to destroy official works.

In [31] Ayei Ibor proposed an entropy-based alert correlation system, E-correlator. Its aim is to strengthen the security of defence infrastructure within cyberspace. It analyses a large set of alerts, and it leads to a minimum loss of the original raw alerts. For this model, original raw alerts serve as input, and for the corresponding alert, it generates a hyperactive alert graph. For building the graph, this model utilized DBSCAN (density-based spatial clustering of applications with noise). Predetermining the number of clusters is not required. For big data, this model results in O(n log n) computational complexity. But it does not consider vulnerabilities in applications, and it cannot be used for multistage attack prediction because its efficacy is limited.

In [32] Krupa proposed an architectural model that used a semi-supervised taxonomy to make an Intrusion Detection System. Using supervised learning requires expert analysts who rely only on labeled data. Here, they combined both labeled and unlabeled data for a better classifier. They used a self-learning semi-supervised slant for IDS. The training statistic is labeled "acquaintance," which serves as input to the system. The approach starts off with labelled training data, which is used for developing an initial supervised classification model. It then guesses the label for unlabeled data, and the system gradually enhances itself. To ensure dependability, entropy is measured for data with predicted labels, which improves model accuracy. It then calculates the threshold; if the threshold is less than 2, then the packet is accepted; otherwise, it will reject the packet.

Sr. No.	Title of Paper	Name of Author	Published Year	Remarks
1.	A survey of cyber-attack detection strategies	James Raiyn	2014	Highlighted the importance of anomaly detection AI-based methods.
2.	An enhanced cyber-attack attribution framework	Nikolaos Pitropakis	2018	NEON model blends multi-source data collection, behavioral surveillance, and forensic analysis; it identifies APT assaults
3.	Threats, protection, and attribution	Leandros Maglaras	2019	Security Information and Event Management (SIEM) is used for digital forensics.
4.	Real-time threat intelligence and adaptive defense mechanism.	Muritala Aminu	2024	Information Sharing and Analysis Centres (ISACs) are used to recognize and mitigate threats.
5.	A survey on various attacks and their classification	M. Uma	2013	Protection of governmental websites and military/ defence websites.
6.	Attack Detection, Prediction, and Prevention.	Ayei Ibor	2018	Give an entropy based alert correlation system and E-correlator.
7.	IDS using Semi-supervised Machine Learning	Krupa A Parmar	2024	Combined both labeled and unlabeled for calculating threshold.

VII. CONCLUSION

This study presented and reviewed several cyberattacks and their detection strategies. Increased use of online services may give rise to greater cyber dangers, including hacking and data theft of government websites, causing the nation to fall behind in its activities. New tools and strategies are needed to keep up with the rapid growth of today. There is a need for enhanced cyber threat identification, driven by the growing quantity of cyber assaults and increasing complexity, which demands adaptive defences. Detecting and preventing data

leaks requires ongoing organizational effort and commitment. Cyber threat intelligence is crucial for proactively implementing countermeasures and establishing a predictive cybersecurity posture. This article outlines some preventative measures and safeguards against cyberattacks. Further study will focus on increasing awareness of cyber risks. The research will also aim to establish methods to ensure that the CIA of data are not violated.

VIII. REFERENCES

[1] D. Kumar, "Emerging Threats in Cybersecurity," *International Journal of Applied and Natural Sciences,* p. 9, 2023.

[2] Fadziso, Takudzwa, Upendar Rao Thaduri, Sreekanth Dekkati, Harshith Desamsetti, "Evolution of the Cyber security Threat," *Digitalization & Sustainability Review,* vol. 3, p. 12, 2023.

[3] Maad M.Mijwil, Omega John Unogwu, Youssef Filali, Indu Bala, "Exploring the Top Five Evolving Threats in Cybersecurity," *Mesopotamian Journal of Cybersecurity,* vol. 2023, pp. 57-63, 2023.

[4] A. Bendovschi, "Cyber-Attacks-Trends,Patterns and Security Countermeasures," *Elsevier B.V.,* p. 8, 2015.

[5] John Hansen Hammer and Gerardo Schneider, "On the Definition and Policies of Confidentiality," *Third International Symposium on Information Assurance and Security.,* p. 7, 2018.

[6] Harley, Kelsey, Cooper, Rodney, "information Integrity : Are We There Yet?," *Association for Computing Machinery,; Association for Computing Machinery(ACM),* vol. 54, no. 2, pp. 1-35, 31 Mar 2022.

[7] Andrey A. Radionov, vadim R. Gasiyarov, "Industrial Control System Cybersecurity Assessment Handling Delay Estimation," *Springer, Cham,* vol. 857, p. 12, 2022.

[8] Hasan Ahmed Salman, Abdulazeez Alsajri, "The Evolution of Cybersecurity Threats and Strategies for Effective Protection," *Peninsula Publishing LLC,* vol. 2023, pp. 1-13, 2023.

[9] P.Rosenzweig, "National Security Threats in Cyberspace," *American Bar Association Standing Committee on Law and National Security and National Strategy Forum,* vol. 1, p. 10, 2013.

[10] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," *International Journal of Network Security,* vol. 15, pp. 390-396, 2013.

[11] S. K. Sakshi Singh, "The Times Of Cyber Attacks," *ACTA Technica Corviniesis,* p. 5, 3 July 2020.

[12] R. K. Neha Kaushal, "Cyber security and The Fifth Generational Cyberattacks," *TIJER International Research Journal,* vol. 10, no. 7, p. 10, July 2023.

[13] B. Watkins, "The Impact of Cyber Attacks on the Private Sector," *MindPoint Group,* p. 11, August 2014.

[14] Kang Leng Chiew, Kelvin Sheng Chek Yong, Choon Lin Tan, "A Survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications,* vol. 106, pp. 1-20, 15 September 2018.

[15] A. Gazet, "Comparative analysis of various ransomware virii," *Journal in Computer Virology,* vol. 6, pp. 77-90, 04 July 2008.

[16] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights,* vol. 1, no. 2, p. 11, 2021.

[17] Tasnuva Mahjabin, Yang Xiao, Wangdong Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation technoques," *International Journal of Distributed Sensor Networks,* 13 December 2017.

[18] Long Cheng, Fang Liu, Danfeng Yao, "Enterprise data breach: causes, challenges, prevention, and future directions.," *WIREs Data Mining and Knowledge Discovery.,* vol. 7, no. 5, p. 11, 2017.

[19] M. Rich, "Understanding and Selecting a Data Loss Prevention," *Websense,* p. 11, 2014.

[20] "Regular expressions openDLP avaiable at: http://code.google.com/p/opendlp/wiki/RegularExpressions," 1 March 2017.

[21] Shapira Y, Shapira B, Shabati A, "Content-based data leakage detection using extended fingerprinting," *CoRR abs,* 2013.

[22] R. M. Snort, "Lightweight intrusion detection for networks," *Proceedings of the 13th USENIX Conference on System Adminstration,* pp. 229-238.

[23] N. Sfetcu, Advanced Persistent Threats in Cybersecurity, MultiMedia Publishing.

[24] S. a. A. M. Quintero-Bonilla, "A New Proposal on the Advanced Persistent Threat," *Applied Sciences,* vol. 10, no. 11, 2020.

[25] M. L. C. T. Yunfei Su, "A Framework of APT Detcetion Based on Dynamic Analysis," in *National Conference on Electrical, Electronics and Computer Engineering*, China, 2015.

[26] W. W. Paul Giura, "A Context-Based detection Framework for Advanced Persistent Threats," in *International Conference on Cyber Security*, Washington, 2012.

[27] J. Raiyn, "A Survey of Cyber Attack Detection Strategies," *International Journal of Security and its Applications,* vol. 8, pp. 247-256, 2014.

[28] E. P. A. G. G. K. R. D. R. Nikolaos Pitropakis, "An Enhanced Cyber Attack Attribution Framework," *International Conference on Trust and Privacy in Digital Business,* pp. 213-228, 2018.

[29] M. A. F. A. D. M. M. H. J. S. R. Leandros Maglaras, "Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures," *Cornell University,* 12 January 2019.

[30] A. A. O. O. Muritala Aminu, "Enhancing Cyber Threat Detection through Real-time Threat Intelligence and Adaptive Defense Mechanisms," *International Journal of Computer Applications Technology and Research,* vol. 13, no. 08, pp. 11-27, 2024.

[31] O. O. F. A. O. Ayei Ibor, "A Survey of Cybersecurity Approaches for Attack Detection, Prediction, and Prevention," *International Journal of Security and Its Applications,* July 2018.

[32] D. R. a. M. B. N. Krupa A Parmar, "Intrusion Detection System Using Semi-supervised Machine Learning," in *Data Science and Intelligent Applications*, V. P. a. H. K. Ketan Kotecha, Ed., 2024, pp. 223-244.

[33] L. Kim, "Ensuring Confidentiality, Integrity, and Availability of Information," *Springer, Cham,* pp. 391-410, 26 July 2022.