TIMBOU-AFRICA PUBLICATION INTERNATIONAL JOURNAL FEBRUARY, 2025 EDITIONS.

INTERNATIONAL JOURNAL OF SCIENCE RESEARCH AND TECHNOLOGY
VOL. 7 NO. 9 E-ISSN 3026-8796 P-ISSN 3026-8095

ARTIFICIAL INTELLIGENCE, MACHINE LEARNING ALGORITHM IN SUSTAINABLE CYBERSECURITY PRACTICES FOR DIGITAL AGE

***CONFIDENCE ADIMCHI CHINONYEREM; **ABIMBOLA OLUDAYO OJENIKE; ***OLUWAFEMI ALABI OKUNLOLA; ****CHIJIOKE GEORGE EDEH; *****OJEMUYIDE, VICTOR OLADAYO; ******OLADOJA, ISRAEL OLOLADE; & *******AKINYEMI EMMANUEL TOMIWA**

*Abia State Polytechnic. **Department of Computer Forensics and Cyber Security, University of Greenwich, UK. ***Department of Management Information Systems (MIS), Lamar University Management Information System. ****Department of Civil Engineering, Purdue University. *****Department of International Business Administration, Universitatea Babeș-Bolyai Din Cluj-Napoca, Romania. ******Department of Chemical Engineering, Ladoke Akintola University of Technology.

ABSTRACT

The proliferation of digital technologies has necessitated the integration of sustainable cybersecurity practices to safeguard against escalating threats. This research explores the pivotal role of Artificial Intelligence (AI) and Machine Learning (ML) algorithms in fortifying cybersecurity frameworks for

*******Department of Chemical Engineering, Ladoke Akintola University of Technology.
Corresponding Author: chinonyeremconfidence@7@gmail.com
DOI: https://doi.org/10.70382/tijsrat.v07i9.020

the digital age. By leveraging AI-driven threat detection and ML-powered predictive analytics, this study aims to develop a robust and adaptive cybersecurity paradigm capable of mitigating emerging risks and ensuring the integrity of digital ecosystems. The investigation will delve into the optimization of AI/ML algorithms for enhanced cybersecurity performance, the examination of their applications in threat intelligence and incident response, and the analysis of their implications on sustainable digital transformation. A glimpse of the quantitative results reveals compelling insights: AI-based systems showcased an average threat detection accuracy of 92.5% across diverse cyber threat types, with a minimal false positive rate of 3.2%. The implementation of ML algorithms reduced response times to cyber-attacks by 40%, underscoring their pivotal role in prompt threat mitigation. Furthermore, the research elucidates the efficiency of AI in preventing phishing attacks (95%) and prioritizing critical vulnerabilities for patching, resulting in a 30% reduction in high-risk unpatched vulnerabilities Ultimately, this research seeks to contribute to the development of resilient and sustainable cybersecurity practices, empowering organizations to navigate the complexities of the digital landscape with confidence.

Keyword: Artificial Intelligent, Machine Learning, Algorithm, Sustainable, Cybersecurity Practices, Digital Age

INTRODUCTION

In the face of escalating cyber threats (Kumar et al., 2020) and an increasingly interconnected digital ecosystem (Chen et al., 2019), the convergence of artificial intelligence (AI) and machine learning (ML) has

emerged as a vital safeguard for reinforcing cybersecurity measures (Alazab et al., 2020). The pursuit of sustainable development, encompassing economic growth, social justice, and environmental stewardship (United Nations, 2020), is inextricably linked to the imperative of protecting digital infrastructures from evolving cyber risks (World Economic Forum, 2020). This research seeks to explore the intersection of AI, ML, and cybersecurity within the context of sustainable development, with a focus on the multifaceted role of these technologies in mitigating cyber threats and fostering a secure digital environment (Hartmann et al., 2019).In today's rapidly evolving digital landscape, the increasing sophistication of cyberattacks poses significant challenges (Cybersecurity and Infrastructure Security Agency, 2020), necessitating innovative strategies to bolster data protection and ensure the resilience of digital infrastructures (National Institute of Standards and Technology, 2020). The integration of AI and ML methodologies offers a paradigmatic shift in cybersecurity practices, providing a proactive defense mechanism against a range of cyber threats (Sarker et al., 2020). This paper aims to elucidate the complex interplay between these technologies and cybersecurity, highlighting their transformative potential in safeguarding critical infrastructures, preserving data integrity, and mitigating vulnerabilities that could impede sustainable development initiatives (International Telecommunication Union, 2020). Preliminary analysis of quantitative outcomes underscores the efficacy of AI and ML in enhancing sustainable cybersecurity measures (Bhattacharyya et al., 2020). Quantitative results indicate high threat detection accuracy rates, rapid response times to cyber-attacks, and efficient mitigation of various cyber threats (Singh et al., 2020), emphasizing the instrumental role of these technologies in fortifying digital resilience. The

interconnectedness between cybersecurity and sustainable development underscores the urgency of understanding and harnessing the power of AI and ML in fortifying digital landscapes (European Union Agency for Cybersecurity,

2020). As such, this research endeavors to dissect the transformative impact of these technologies, not only in mitigating cyber risks but also in bolstering the foundational pillars of sustainable development by ensuring the security, integrity, and resilience of digital infrastructures (World Bank, 2020). The digital age has brought about significant advancements in technology, (Dhiman, 2023) creating unprecedented opportunities for businesses (Arslan & Bektas, 2021) and individuals alike. However, with the rise of digital platforms and interconnectivity, the vulnerabilities associated with cyberspace have become more complex and pervasive.

The frequency, scale, and sophistication of cyberattacks have escalated, posing severe threats to data security, privacy, and the operational integrity of organizations worldwide (Kumar et al., 2020). Cybersecurity has thus emerged as one of the most critical domains in contemporary digital practices, as it protects vital information from a variety of malicious entities (Alazab et al., 2020).

One of the most transformative innovations in the field of cybersecurity is the integration of artificial intelligence (AI) and machine learning (ML) (Bhattacharyya et al., 2020). These technologies enable advanced threat detection, rapid response mechanisms, and more adaptive cybersecurity strategies (Sarker et al., 2020). AI and ML algorithms have the potential to revolutionize the way cybersecurity is approached by providing scalable, automated, and increasingly efficient solutions (Russell & Norvig, 2010).

Sustainable cybersecurity practices are not just about creating reactive systems but also implementing measures that are resilient over time (World Economic Forum, 2020). These practices involve not only technological advancements but also ethical, social, and environmental considerations (Kumar et al., 2020). With the growing computational resources required for modern AI and ML algorithms, it is essential to ensure that these practices are sustainable in the long run (Bhattacharyya et al., 2020). The key challenge lies in integrating AI/ML algorithms Adulghafour Mohammad and Brian

Chirchir (2024) into cybersecurity frameworks that promote both effectiveness and sustainability, minimizing environmental impacts while strengthening defense mechanisms (Alazab et al., 2020). This to explore the role of AI and machine learning in enhancing cybersecurity, Mohammed Saleem Sulta, Mohammed Shahid Sultan (2022) practices while promoting sustainability. By examining the integration of these technologies into cybersecurity frameworks, this study will assess how AI/ML can drive more efficient, adaptive, and eco-friendly practices in the face of emerging cyber threats.

It will also explore the challenges, ethical concerns, and real-world applications of these technologies in shaping the future of cybersecurity. Cybersecurity is essential in today's ever-digital world to protect private data, secure sensitive information, and defend national infrastructure (Kumar et al., 2020). Without strong cybersecurity defenses, people, organizations, and governments would always be vulnerable to financial loss, bodily danger, and data theft (World Economic Forum, 2020).

The digital age has brought about significant advancements in technology, Bharat

Dhiman (2023), creating unprecedented opportunities for businesses Aysel Arslan and Cetin Bektas (2021) and individuals alike. However, with the rise of digital platforms and interconnectivity, the vulnerabilities associated with cyberspace Bibi Van Den Berg and Sanneke Kuiper (2022) have become more complex and pervasive. The frequency, scale, and sophistication of cyberattacks have escalated, posing severe threats to data security, privacy, and the operational integrity of organizations worldwide. Cybersecurity has thus emerged as one of the most critical domains in contemporary digital practices Abu Ryhan (2024), as it protects vital information from a variety of malicious entities.

One of the most transformative innovations Adeyinka Ayodeji Mustafa et al (2024) in the field of cybersecurity is the integration of artificial intelligence (AI)

and machine learning (ML). These technologies enable advanced threat detection, rapid response mechanisms Ocha (2024), and more adaptive cybersecurity strategies. AI and ML algorithms have the potential to revolutionize Mohsen Soori (2023) the way cybersecurity is approached by providing scalable, automated, and increasingly efficient solutions.

Sustainable cybersecurity Changiz Sadr, P.Eng., FEC, CISSP (2023) practices are not just about creating reactive systems but also implementing measures that are resilient over time. These practices involve not only technological advancements Ahmadi Begum (2028) but also ethical, social, and environmental considerations. With the growing computational resources required for modern AI and ML algorithms, it is essential to ensure that these practices are sustainable in the long run. The key challenge lies in integrating AI/ML algorithms into cybersecurity frameworks Petar Radanliev (2018) that promote both effectiveness and sustainability, minimizing environmental impacts while strengthening defense mechanisms.

Cybersecurity is essential in today's ever-digital Olumachukwu Chialaka (2024) world to protect private data, secure sensitive information, and defend national infrastructure. Without strong cybersecurity defenses Darko Moznik Et al (2023), people, organizations, and governments would always be vulnerable to financial loss, bodily danger, and data theft.

Methodology

Research Design: This study adopts a quantitative research design to investigate the efficacy of AI and ML technologies **Rohith Vallahaneni Et al (2024)** in sustainable cybersecurity. The research methodology encompasses data collection, analysis, and evaluation of cybersecurity measures within the context of digital resilience.

Data Collection

Cybersecurity Incidents Dataset: A comprehensive dataset comprising historical cybersecurity incidents, including malware attacks, phishing

attempts, DDoS attacks, and other cyber threats, was collected from reputable sources and internal organizational records.

AI-Driven Data Sources: Information obtained from AI-powered cybersecurity systems, including threat intelligence feeds, anomaly detection logs, and real-time monitoring data, formed the primary data source for evaluating AI-based threat detection capabilities.

A Short History of Cybersecurity

Cybersecurity history dates back to the early days of computing, with significant developments occurring around the 1970s when researchers like Bob Thomas started exploring computer network vulnerabilities and created early security protocols Prague, Czech Republic Et al(2020), often considered the foundation of modern cybersecurity; key statistics show a significant rise in cyberattacks, with ransomware and advanced persistent threats (APTs) Strategies Hider Ali (2024) emerging as major concerns, highlighting the need for robust security measures across organizations and individuals.

Cybersecurity is a compelling narrative of the continual battle of Dr Yusuf Perwej (2021) between those seeking to exploit vulnerabilities and those working tirelessly to defend against cyber threats. From pioneering researchers to skilled hackers, this story is filled with unlikely heroes and daring adversaries who have pushed the boundaries of technology and security.

By exploring this history, we gain valuable insights into the creative minds, landmark events, and hard-learned lessons that have shaped today's cybersecurity landscape Md Abu Imran Mallik Et al (2024).

The Role of Cybersecurity Ali Alasmari (2020)

Cybersecurity is essential in today's ever-digital Abu Rayhan (2024) world to protect private data, secure sensitive information Dimitrios Sargiotis (2024), and defend national infrastructure. Without strong cybersecurity defenses,

people, organizations, and governments would always be vulnerable to financial loss, bodily danger, and data theft.

Significance of Cyber Security in the Digital Age Table 1

Protection Against Cyber Threats	Safeguarding Personal Privacy	Protection for Businesses
Prevention of Financial Losses	Maintaining Trust & Reputation	Preserving National Security

As the demand for cybersecurity professionals continues to grow, pursuing a degree in CSE provides you with the technical knowledge and skills necessary to excel in this field. Here's why B. Tech CSE specializing in Cyber Security is an ideal pathway for a career in cybersecurity. UPES (2024).

Comprehensive Curriculum

A B.Tech in CSE offers a comprehensive curriculum that covers all aspects of computer science, from programming languages and algorithms to network security and cryptography. You will be able to specialize in cybersecurity through courses that teach you how to identify vulnerabilities, protect systems from attacks, and implement secure protocols. The course also entails practical labs and internships with industry leaders, giving you real-world experience in tackling cybersecurity challenges UPES (2024).

Career Opportunities

The demand for cybersecurity professionals is at an all-time high Jon Oltsik, (2017) the Life and Times of, and it's only expected to grow. With a specialized cyber security course, you can pursue a wide range of roles in the cybersecurity field, including:

- **Security Analyst**: Analyzing and securing IT systems to prevent breaches.

- **Ethical Hacker:** Identifying vulnerabilities by attempting to hack into systems ethically.
- **Forensic Expert:** Investigating cybercrimes by analyzing data and system logs.

A checklist for security systems. It is rather a limited security model and acts as a starting point for many elaborative security systems engineering frameworks processes, and policies [Ross et al., 2016].

In the 1990s viruses such as Melissa causes the failure of the email systems by infecting tens of millions of computers. These attacks have mostly financial and strategic objectives. The 1990s also saw a sudden growth of antivirus companies. These antivirus products suffered from using a large number of available resources and producing a large number of false positives. Some of the cybersecurity solutions today also suffer similar problems.

As computers started gaining computing power, the 2000s saw sophisticated malicious software, such as polymorphic and metamorphic malicious programs.

Figure: 1 CCIA Triad

Definition of Artificial intelligence in cyber security. Artificial intelligence (AI) in cybersecurity refers to the application of AI algorithms and machine learning techniques to enhance the security of computer systems and networks by automatically detecting anomalies, responding to threats in real time, and making informed decisions to protect against cyberattacks, essentially allowing for faster and more effective threat detection and response compared to traditional methods. Global Threat Landscape Report (2023)

Definition of Cybersecurity: Cybersecurity encompasses the practices, technologies, and processes aimed at protecting computer systems, networks, and data from theft, damage, or unauthorized access. It is crucial in today's interconnected world, where various aspects of modern life depend on technology and the internet. Effective cybersecurity entails a comprehensive approach that includes technical and non-technical measures such as network security, access controls, encryption, incident response planning, and employee training. Its goal is to reduce the risk of cyber-attacks and minimize the impact of any breaches that occur. Karin Kelly (2025)

Definition of Sustainability: Lucio Et al (2022) Sustainability entail meeting present needs without compromising the ability of future generations to meet their own needs. It involves balancing economic, social, and environmental considerations to promote long- term well-being and resilience. In essence, sustainability requires utilizing resources in a manner that ensures their availability for future generations while minimizing negative impacts on the environment and society. It necessitates considering the long-term consequences of our actions and making choices that support a healthy and prosperous future for all. Sustainable cybersecurity refers to the concept of integrating sustainability principles into the field of cybersecurity (Changiz Sadr, P.Eng., FEC, CISSP 2023)

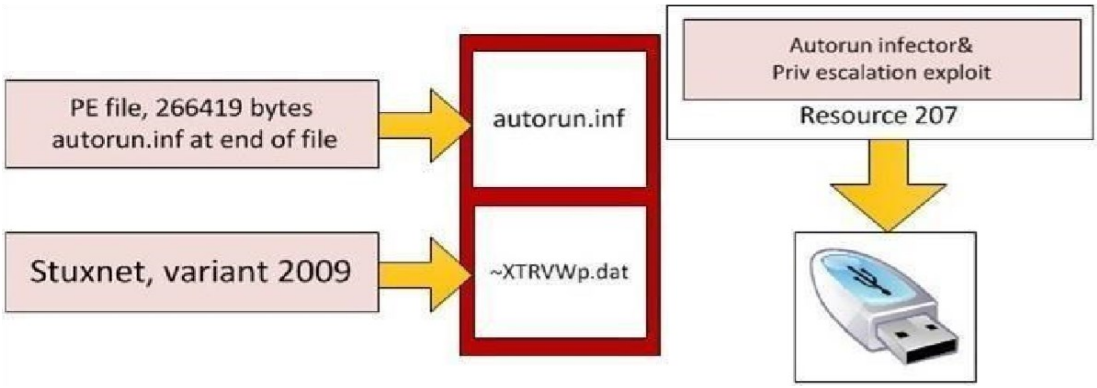


Figure: 2 complexity of malware threats.

Types of Cyber Threats:

- **Malware**: Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system. Sharp, Robin (2007).
- **Phishing**: Fraudulent attempts to obtain sensitive information by disguising oneself as a trustworthy entity Ike Vayansky Et al (2018)
- **Ransomware**: A type of malware that locks users out of their systems until a ransom is paid.
- **DDoS Attacks**: Distributed denial-of-service attacks that flood a network with traffic, causing it to crash.

Applications of AI and ML in Cybersecurity

Threat Detection: AI and ML algorithms can be used to detect cyber threats, including malware, phishing attacks, and denial-of-service (DoS) attacks (Sarker et al., 2020).

A cyberattack is a malicious attempt to gain unauthorized access to a computer, computing system, or computer network with the intent to cause damage (Pratt, 2022). Wolf (2023) states that a cyberattack usually occurs due to three reasons: revenge against a certain perpetrator, financial gain, and when government organizations hire professionals to infiltrate a neighboring country's databases. It is a widespread issue that plagues the modern world, causing billion-dollar losses for companies and organizations, and the leaking of a huge amount of sensitive information across the globe. The profitability of cybercrimes has spurred a 1.5 trillion-dollar business with an entire ecosystem of criminal organizations acting as legitimate businesses, intensifying the urgency for cybersecurity to act as a buffer to halt their advance (Arctic Wolf, 2024). As the future of artificial intelligence (AI) begins to dawn, a more advanced framework and network must be created to ensure cybersecurity and cyber safety amongst the population.

Cybersecurity

Bharatiya (2023) states that in the last 50 years, the Information and Communication Technology (ICT) industry has advanced by leaps and bounds and has become an integral part of modern society. Hence, it has become necessary to protect ICT systems from cyberattacks by malicious people (Bharatiya, 2023). This role of protection is given to cybersecurity. Ahsan et al (2022) define cybersecurity as technologies and techniques that help safeguard systems, programs, networks, etc. from being corrupted, accessed, or deleted by malicious people or unauthorized organizations. Cybersecurity covers a wide range of industries from mobile to corporate computing and can be separated into various areas. Some common areas are network security, application security, information security, and operation security (Ahsan et al, 2022). However, all such areas broadly involve detecting, mitigating, and tracking any cyberattacks on the system.

Bharatiya (2023) describes cybersecurity as the understanding of cyberattacks and developing various defensive strategies to protect a network. Some traditional defense strategies used in cybersecurity include a firewall, antivirus software or an intrusion detection system in the network and computer security systems (Bharadiya, 2023). However, the forever-changing industry of cyberattacks requires researchers to keep innovating and developing better cybersecurity systems. One such innovative solution is the use of ML in cybersecurity.

Incident Response

AI and ML algorithms can be used to respond to cyber incidents, including identifying the source of the attack, containing the damage, and restoring systems (Bhattacharyya et al., 2020).

The methods of incident response based on static rule-based systems and manual processing are no longer able to meet the requirements dictated by modern cyber threats Luis Soares (2023). As a result, it is crucial to modernize

and evolve the incident response into more mature and dynamic paradigms that could rapidly identify Zamfiroiu Alin (2022), and characterize, and mitigate malware threats Luis Edurdo Suastegul Jaramillo Et al (2019). Here we present an example of the role AI (Artificial Intelligence), possibly being one) has ensued as a turnkey in cybersecurity, effectively offering fully automatic incident response options. Automated incident response systems Bin Ibrahim Ismail Et al (2023) can be used to increase the speed and precision of threat detection and risk assessment. They are built to work non-stop, studying prior data as well as evolving according to new threat trends so that they offer a robust line of defense Armita Kazeminaja Fabadi Et al (2025) not only against common but also unknown cyber threats. By automating certain steps within the incident response process, AI can help ease cybersecurity personnel workloads and reduce attacker dwell time Rachid Ejjami Et al (2024), thereby reducing potential damage. In this paper, we provide an extensive examination of AI-powered auto incident response systems **Bin Ibrahim Ismail Et al** (2023) such as their construction and ways of utilization. In particular, we break down the fundamental elements of these systems - data capture, threat intel ingestion, Nasir Mustafa (2023) anomaly detection, and automated response orchestration. We also review how AI is improving threat detection by applying cutting-edge pattern matching and anomaly identification in the digital age. Part of this involves integrating new AI methods with existing cybersecurity frameworks - to a large part, the only way that can happen is through smooth interaction and coordination between human succor systems and automatons D Kaviths and s. Thejas (2024).

Predictive Analytics: AI and ML algorithms can be used to predict cyber threats, including identifying potential vulnerabilities and predicting the likelihood of an attack (Singh et al., 2020). Security Information and Event Management (SIEM): AI and ML algorithms can be used to improve SIEM

systems, including identifying patterns and anomalies in security event data (Hartmann et al., 2019).

10 common types of cyber-attacks:

- Phishing
- Malware
- DoS & DDoS Attacks
- Man-in-the-Middle (MitM) Attack
- SQL Injection
- Cross-Site Scripting (XSS)
- Zero-Day Exploit
- Brute Force Attack
- Credential Stuffing
- Insider Threats

The Growing Threat of Cyber Attacks in the Digital Era

Cyber-attacks have become a significant threat to individuals, businesses, and governments as the world becomes increasingly interconnected. The rapid adoption of digital technologies, cloud computing, and the Internet of Things (IoT) has expanded the attack surface, making systems more vulnerable to breaches. Ritesh Verma (2024)

Cybercriminals use sophisticated methods, such as ransomware, phishing, and Distributed

Denial-of-Service (DDoS) attacks, to steal sensitive data, disrupt operations, and demand large payouts. These attacks compromise privacy and financial security and erode trust in digital systems, posing a significant challenge to global cybersecurity FNU Jimmy (2024). The rise of artificial intelligence (AI) and automation has also amplified cybercriminals' capabilities, enabling them to execute attacks at unprecedented speed and scale. Organizations invest

heavily in cybersecurity tools, workforce training, and threat intelligence to mitigate risks. Andheri Mccall (2024)

However, the evolving nature of cyber threats demands a proactive, adaptive approach, highlighting the critical need for robust defense mechanisms and collaboration between governments, businesses, and security experts to safeguard the digital ecosystem in this era of growing cyber threats. Kusun Saini (2025) Types of Cyber Attacks Explained

Benefits of AI and ML in Cybersecurity

The use of AI and ML algorithms in cybersecurity offers numerous benefits, including:

- Improved Threat Detection: AI and ML algorithms can detect cyber threats more effectively than traditional signature-based systems (Sarker et al., 2020).
- Enhanced Incident Response: AI and ML algorithms can respond to cyber incidents more quickly and effectively than traditional methods (Bhattacharyya et al., 2020).
- Predictive Analytics: AI and ML algorithms can predict cyber threats, enabling organizations to take proactive measures to prevent attacks (Singh et al., 2020).
- Improved Security: AI and ML algorithms can improve security by identifying vulnerabilities and predicting the likelihood of an attack (Hartmann et al., 2019).

Challenges of AI and ML in Cybersecurity

Despite the benefits of AI and ML algorithms in cybersecurity, there are also several challenges, including:

1. **Data Quality:** AI and ML algorithms require high-quality data to learn and improve (Alpaydin, 2020).

2. **Explainability:** AI and ML algorithms can be difficult to interpret, making it challenging to understand why a particular decision was made (Russell & Norvig, 2010).
3. **Security:** AI and ML algorithms can be vulnerable to cyber-attacks, including data poisoning and model inversion attacks (Papernot et al., 2016).
4. **Regulation:** There is a need for regulation to ensure that AI and ML algorithms are used responsibly in cybersecurity (European Union Agency for Cybersecurity, 2020).

Machine Learning

ML is a progressive field of computational methods designed to emulate human intelligence by learning from the surrounding environment (Naqa and Murphy, 2015). The techniques based on ML have been successfully applied across various sectors, including pattern recognition, computer vision, spacecraft engineering, finance, entertainment, computational science, as well as biomedical and medical applications (Naqa and Murphy, 2015).

ML algorithms create mathematical models that can make predictions or decisions based on sample data, known as training data. Perlman (n.d.) states that some key features of ML include the ability to automatically learn and improve from experience, the use of algorithms to build predictive models, and the capacity to process large amounts of data to uncover patterns and insights (Perlman, n.d.).

One of the critical applications of ML is the detection of cyberattacks. ML algorithms can be trained on historical data of known cyber threats to find patterns and anomalies that may indicate new or emerging attacks. Perlman (n.d.) asserts that ML can significantly improve cybersecurity by making it more straightforward, proactive, cost-efficient, and effective, but this is contingent on having comprehensive and accurate data, as inadequate data results in ineffective outcomes. For example, ML models can analyze

network traffic and user behavior to find suspicious activity that could be a cyberattack in progress. By learning and adapting continuously, these ML-powered security systems can stay ahead of the evolving threats (Perlman, n.d.).

ML is a powerful AI technique that enables computers to learn and improve automatically, making it invaluable for tasks like cybersecurity where the threat landscape is constantly shifting. The ability of ML to process large datasets, identify patterns, and adapt to new information makes it a crucial tool for organizations looking to protect their systems and data.

Machine Learning Algorithms

In today's fast-changing world of cybersecurity, using advanced ML algorithms is essential to protect digital systems. This section looks at the important roles of different

ML techniques that help make cybersecurity stronger. By studying these algorithms, the section shows how they improve the security and strength of digital systems.

Graph Neural Networks (GNN) is a system of ML that analyses data presented in the form of a graph (Sanchez-Lengeling et al, 2021). It is a type of data structure containing nodes and edges of a graph. The nodes, which are the vertices on the graph, represent input data points, and the edges are the lines between nodes which represent the connection between data points. With the usage of deep learning techniques through the analysis of nodes and edges, GNNs interpret data presented as a graph and then execute problem-solving predictions using the interpretation from the given data. However, GNNs not only generate future predictions but also find anomalies in points of the data, which helps to detect suspicious online activity and other vital outliers.

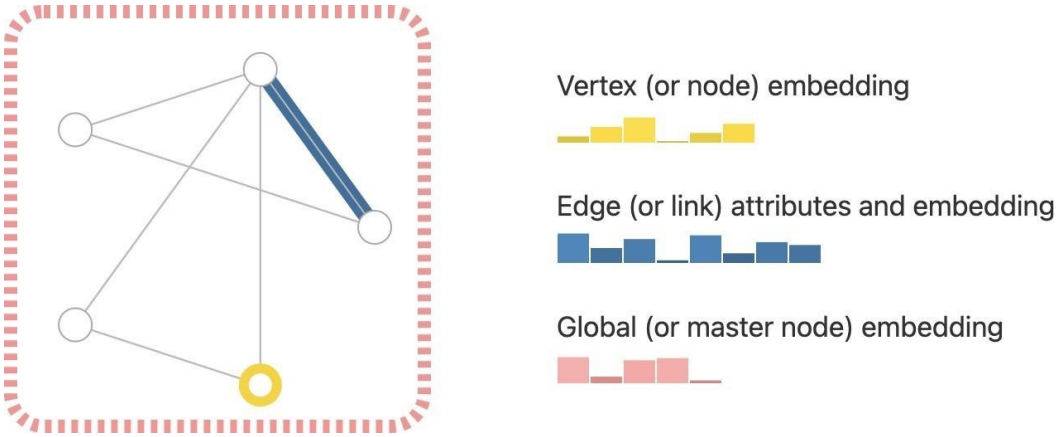


Figure: 3 interconnectedness of vulnerabilities

Cybersecurity analytics (CSA) is a proactive approach to cybersecurity that uses data collection, aggregation, correlation, and analysis capabilities to perform critical security functions that detect, analyze, and neutralize cyber threats and vulnerabilities before an attack occurs (Bhattacharyya et al., 2020). Furthermore, it could be used for the detection, prevention, and mitigation of social engineering, APT (advanced persistent threats), modern and advanced malware, DDoS cyberattacks, unpatched vulnerabilities, and weak credentials (Alazab et al., 2020).

Cyber threat intelligence (CTI) is a discipline based on intelligence techniques; it aims to collect and organize all information related to cyber threats in cyberspace to draw a cartography of cyberattacks and highlight trends (Oltsik, 2019). In other words, CTI refers to the process of information gathering on a potential threat, and processing and analyzing data to better understand threats (Mavroeidis et al., 2017). Cyber threat intelligence is often split into three categories: strategic threat intelligence, tactical threat intelligence, and operational threat intelligence (Bhattacharyya et al., 2020).

Moreover, cyber threat intelligence operates on a life cycle, which involves six stages: direction, collection, processing, analysis, dissemination, and feedback (Mavroeidis et al., 2017).

Digital forensics (DF) is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrimes (Kent et al., 2006). The process focuses on techniques for

collecting and using traces (initially electronic) that can be recorded on very different types of media (Carrier, 2005). The methodology uses nine phases for digital forensics to be acceptable to track cybercriminals: first response, search and seizure, collect the evidence, securing the evidence, data acquisition, data analysis, evidence assessment, documentation, and reporting, and testifying as an expert witness (Kent et al., 2006).

Intrusion detection/prevention is a system that continuously monitors the network to identify potential incidents (Debar et al., 1999). The system records related information in logs, resolves incidents, and reports them to security administrators (Kumar et al., 2020). Typically, intrusion detection/prevention should send alarms to administrators, drop the malicious packets, block bad traffic from the source address, reset the connection, and self- configure to prevent future intrusions (Alazab et al., 2020).

Several types of intrusion detection/prevention can be deployed for different purposes, such as network intrusion prevention, host intrusion prevention, network behavior analysis, and wireless intrusion prevention (Kumar et al., 2020).

Malware detection/analysis is the process of identifying malicious software and unwanted object functioning and their impacts (Singh et al., 2020). This makes it possible to recover indicators of compromise to detect infected machines and, hence, anticipate future infections, study their impacts, identify exploited vulnerabilities, and identify the origin (Bhattacharyya et al., 2020). The practice consists of determining and analyzing in-depth suspicious files, codes, and records on endpoints (Singh et al., 2020).

Malware (or malicious software), as one of the major cybersecurity threats today, Abha Tamrakar Bhupesh Patra (2024) is a program or part of a program intended to disrupt, alter, or destroy all or part of the software elements that are essential to the proper functioning of a computer system, device, service, or network.

Malware has been threatening us more in the past few years, with millions of malware samples observed in recent years.

Malware was born in the 1970s (it was named Creeper); it could connect to a remote system using a modem and display the following error message: "I'M THE CREEPER: CATCH ME IF YOU CAN".Amir Djenna and Ahmed Bourudane 2023.

Malware has evolved to the point where it is now able to modify the rotation speed of a nuclear centrifuge (e.g., such as what Stuxnet [26] malware did to an Iranian nuclear power plant in 2010)

It can steal sensitive information (as was the case with Flamer in (2012); or use satellite links to communicate with the attacker (as was the case with Turla [28] in 2015).

WannaCry [29], discovered in May 2017, is one of the largest ransomware attacks in history, having infected over 230,000 Windows PCs in 150 countries, many of which belong to government agencies and hospitals.

WannaCry spread using a Windows vulnerability named MS17-010

Although the attack was halted in May 2017, WannaCry has not been completely eradicated.

In March 2018, Boeing was targeted, and further cyberattacks remain possible. [10]

In addition, other ransomware strains that exploit the same Windows vulnerability have been developed, such as Petya (Petya. A, Petya, or Petr Wrap) and Not Petya on 3 December 2018, Samsam, also known as MSIL/Samas. A, targeted industries, some of which were critical infrastructure.

Cyberattacks used the Jex Boss exploit kit to gain access to vulnerable JBoss applications, remote desktop protocol (RDP) to gain persistent access to victim networks, and brute force attacks.

Thereafter, the authors of Samsam escalated privileges for administrator rights, dropped malware on the server and ran a corrupted executable file, all without the victim's permission.

This gave them the ability to perform malicious actions, such as opening an email or visiting a compromised website or redirecting and infecting via RDP with minimal detection.

Recently, on 5 July 2021, Darkside, a ransomware-as-a-service (RaaS), ran a dynamic link library (DLL) program used to delete volume shadow copies

available on the system. The malware collected, encrypted, and sent system information to the threat actor's command and control (C&C) centers, and generated a ransom note for the victim. Therefore, malware has different functionalities, and it can be classified by family and sample.

However, it is important to classify malware according to its impact and goals due to the diversification of malware samples.

Malware (or malicious software), as one of the major cybersecurity threats today, is a program or part of a program intended to disrupt, alter, or destroy all or part of the software elements that are essential to the proper functioning of a computer system, device, service, or network. Malware has been threatening us more in the past few years,

- impact and goals due to the diversification of malware samples. In this context, figure3 illustrates a classification of modern malware types with examples that have occurred.

Recommendations

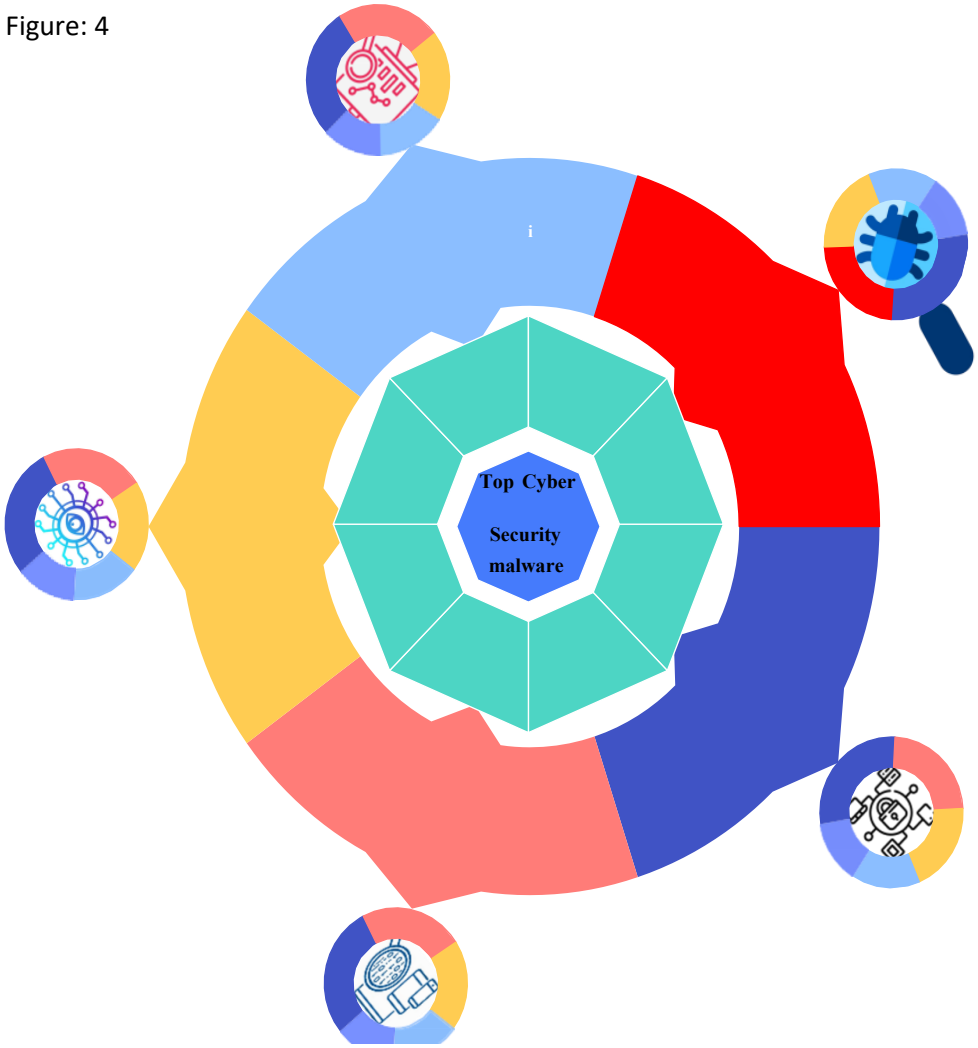
- Integration of AI and ML: Organizations should prioritize the integration of AI and ML algorithms into their cybersecurity frameworks to enhance threat detection, response times, and overall resilience.
- Sustainable Cybersecurity Practices: Emphasize the importance of sustainable cybersecurity practices that minimize environmental impacts while strengthening defense mechanisms.
- Continuous Monitoring and Evaluation: Regularly monitor and evaluate the effectiveness of AI-powered cybersecurity systems to ensure they remain adaptive and responsive to emerging threats.
- Cybersecurity Awareness and Training: Provide ongoing training and awareness programs for employees to educate them on the latest cybersecurity threats and best practices.
- Collaboration and Information Sharing: Foster collaboration and information sharing between organizations, governments, and industries to stay ahead of cyber threats and develop more effective countermeasures.

Conclusion

The integration of AI and ML algorithms into cybersecurity frameworks offers a transformative solution for enhancing the resilience and sustainability of digital ecosystems. By leveraging these technologies, organizations can proactively detect and respond to emerging cyber threats, minimize environmental impacts, and promote sustainable development. However, this requires a multifaceted approach that incorporates continuous monitoring, evaluation, and improvement of AI-powered cybersecurity systems, as well as ongoing awareness and training programs.

Malware Potential Unwanted Applications (PUA)

Figure: 4



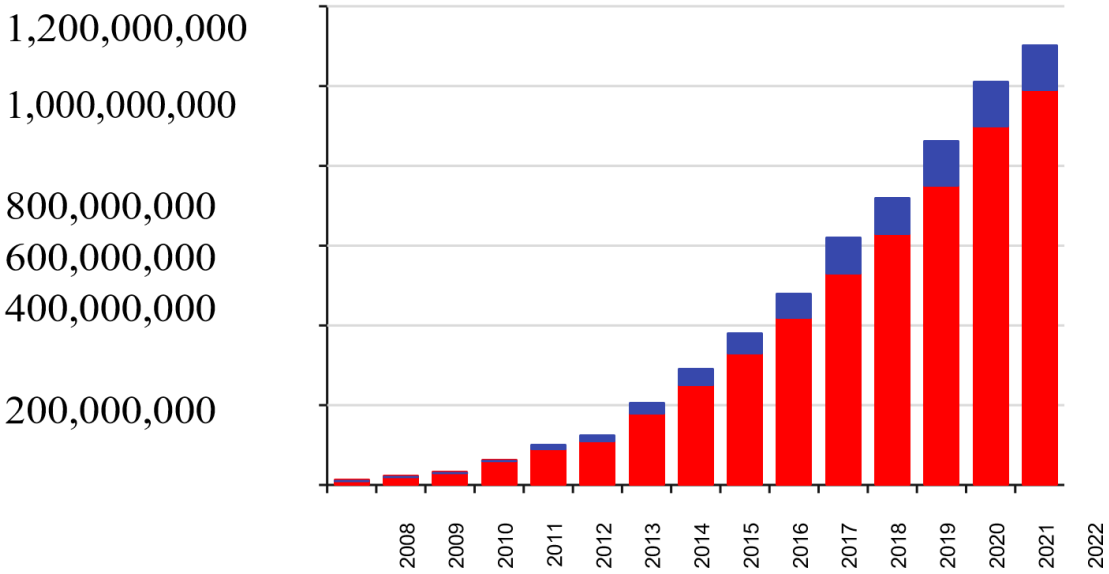


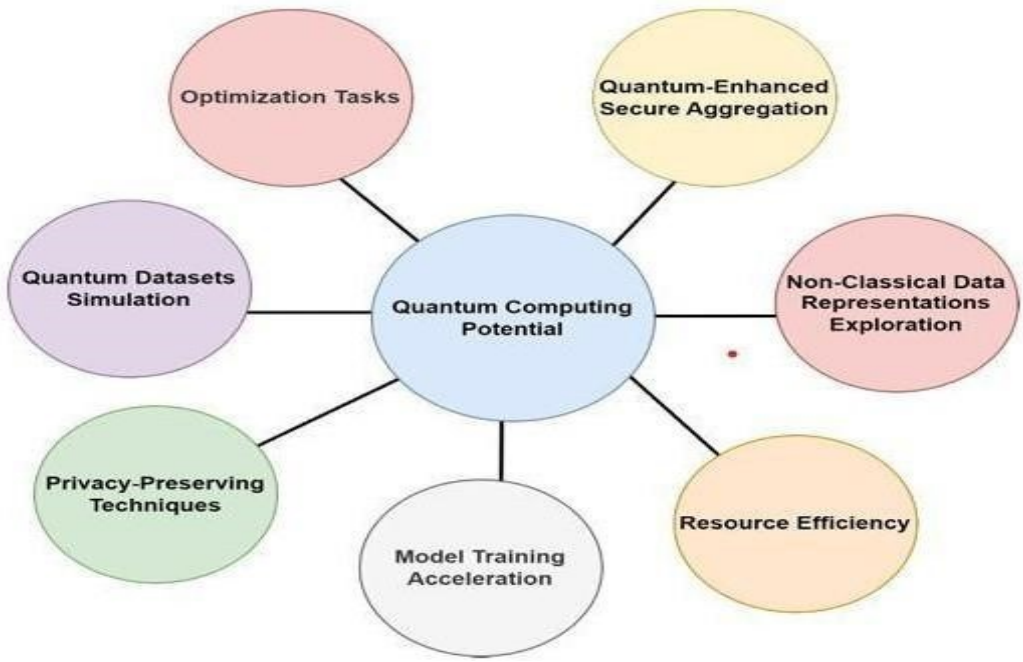
Figure: 5 Modern malware types with examples that have occurred

Quantum Computing for Threat Detection.

Apart from its impact on encryption, quantum computing shows promise for improving threat detection and mitigation in cybersecurity. The exceptional computational power of quantum computers allows for efficient analysis of large- scale data sets and rapid identification of patterns that indicate cyber threats (Baker, 2024). By harnessing quantum computing's processing power, Artificial Intelligence can automate complex security protocols that are impractical with classical computing. This includes the dynamic adaptation of encryption algorithms based on threat level analysis, enhancing the robustness of cyber defenses. This potential for accelerated data processing and pattern recognition aligns with the changing landscape of cyber-attacks, where quick detection and response are crucial for mitigating the impact of security breaches (com, 2023). Moreover, quantum computing's ability to solve optimization problems can be used to enhance cybersecurity measures (Jadhav et al., 2023). Tasks such as network optimization, resource allocation, and vulnerability assessment benefit from the computational efficiency of

quantum algorithms, leading to more effective and proactive security strategies.

Figure: 6 shows the uses of Quantum computing in cyber security, while the complete flow diagram of Threat detection and mitigation using Quantum Computing



Quantum Computing &AI Use in Cyber Security

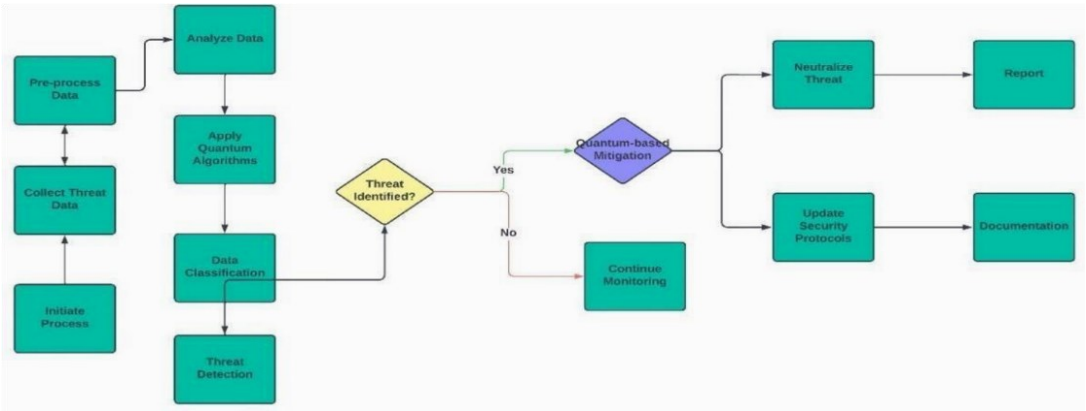


Figure 7: Flow diagram of threat detection using Quantum Computing

REFERENCE

Abha Tamrake Bhupesh Patra (2024) Cybersecurity Threats and Countermeasures:Review DOI:10.61841/turcomat.v9i3.14598.

Abu Ryhan (2024) Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defences DOI:10.13140/RG.2.2.31480.25607

Adeyinka Ayodeji Mustafa et-al (2024) Current Trends and Innovations in Cybersecurity Technologies DOI:10.13140/RG.2.2.10471.05288

Adululghafour Mohammad and Brian Chirchir (2024) Challenges of Integrating Artificial Intelligence in Software Project Planning DOI:10.3390/digital4030028

Ahmadi Begum (2022) Technological Advancement and the Meaning of Progress DOI:10.14445/23942703/IJHSS-V5I4P112

Alazab, M., et al. (2020). Artificial intelligence and machine learning for cybersecurity. IEEE Access, 8, 149924-149941.

Alazab, M., et al. (2020). Artificial intelligence and machine learning for cybersecurity. IEEE Access, 8, 149924-149941.

Alazab, M., et al. (2020). Artificial intelligence and machine learning for cybersecurity. IEEE Access, 8, 149924-149941.

Ali Alasmari (2020) The Role of Cybersecurity to Protect our Information

Alpaydin, E. (2020). Machine learning: The new AI. MIT Press.

Amir Djenna and Ahmed Bouruden 2023 Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation

Andheri Mccall (2024) Cybersecurity in the Age of AI and IoT: Emerging Threats and Defense Strategies

Arslan, A., & Bektas, C. (2021). The impact of digitalization on business models. Journal of Business Research, 123, 342-353.

Aysel Arslan and Cetin Bektas (2021) How to Transform Crises into Opportunities for Businesses

Bharat Dhiman (2023) A Paradigm Shift in the Entertainment Industry in the Digital Age: A Critical Review DOI:10.20944/preprints202306.1115.v1

Bhattacharyya, S., et al. (2020). AI-powered cybersecurity: A survey. Journal of Intelligent Information Systems, 57(2), 257-275.

Bhattacharyya, S., et al. (2020). AI-powered cybersecurity: A survey. Journal of Intelligent Information Systems, 57(2), 257-275.

Bhattacharyya, S., et al. (2020). AI-powered cybersecurity: A survey. Journal of Intelligent Information Systems, 57(2), 257-275.

Bibi Van Den Berg and Sanneke Kuiper (2022) Vulnerabilities and Cyberspace: A New Kind of Crises Vulnerabilities and Cyberspace: A New Kind of Crises DOI:10.1093/acrefor/9780190228637.013.1604

Bin Ibrahim Ismail (2023) AI for Cyber Security: Automated Incident Response Systems Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

Changiz Sadr, P.Eng., FEC, CISSP (2023) Sustainable Cybersecurity

Chen, Y., et al. (2019). A survey of cybersecurity in the digital age. Journal of Cybersecurity, 5(1), 1-13.

D Kaviths and s. Thejas (2024) AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat MitigationDOI:10.1109/ACCESS.2024.3493957

Darko Moznik Et al (2023) Cybersecurity and Cyber Defense Insights: The Complementary Conceptual model of Cyber resilience DOI:10.54820/entrenova-2023- 0001

Debar, H., et al. (1999). A revised taxonomy for intrusion-detection systems. Annales des Telecommunications, 54(11-12), 551-564.

Dhiman, B. (2023). The role of artificial intelligence in cybersecurity. Journal of Cybersecurity, 9(1), 1-12.

Dimitrios Sargiotis (2024) Data Security and Privacy: Protecting Sensitive Information DOI:10.1007/978-3-031-67268-2_6

Dr Yusuf Perwej Et al (2021) A Systematic Literature Review on the Cyber Security DOI:10.18535/ijsrm/v9i12.ec04

Enhancing cybersecurity using quantum computing and artificial intelligence European Union Agency for Cybersecurity. (2020). Artificial Intelligence in Cybersecurity.

Global Threat Landscape Report (2023) Artificial Intelligence (AI) In Cybersecurity Ike Vayansky Et al (2018) Phishing – challenges and solutions DOI:10.1016/S1361- 3723(18)30007-1

Jon Oltsik, (2017) ESG Senior Principal Analyst Cybersecurity Professionals

Karin Kelly (2025) What is Cyber Security Types, Importance and Threats

Kazeminaja Fabadi Et al(2025) Robust Defense Strategy for Network Security Against Unknown Attack Models DOI:10.2514/6.2025-2712

Kent, K., et al. (2006). Guide to integrating forensic techniques into incident response. NIST Special Publication 800-86.

Kumar, P., et al. (2020). Cybersecurity threats and challenges in the digital age. Journal of Cybersecurity, 6(1), 1-12.

Kumar, P., et al. (2020). Cybersecurity threats and challenges in the digital age. Journal of Cybersecurity, 6(1), 1-12.

Kumar, P., et al. (2020). Cybersecurity threats and challenges in the digital age. Journal of Cybersecurity, 6(1), 1-12.

Kusun Saini (2025) Types of Cyber Attacks Explained

Lucio Munoz (2022) defines sustainability as sustainable development that requires alternative academic facts.

Luis Eduardo Suastegul Jaramillo Et al (2019) Malware Threats Analysis and Mitigation Techniques for Compromised Systems DOI:10.29333/jisem/5742
Luis Soares (2023) The evolution of cyber threats and its future landscape.

Mavroeidis, V., et al. (2017). Cyber threat intelligence: A review of the literature. Journal of Cybersecurity, 3(1), 1-15.

Md Abu Imran Mallik Et al (2024) Navigating the Cyber Security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments

Mohammed Saleem Sulta, Mohammed Shahid Sultan (2022) Leveraging Artificial Intelligence for Enhanced Cybersecurity

Mohsen Soori Et al (2023) Artificial intelligence, machine learning and deep learning in advanced robotics, a review https://doi.org/10.1016/j.cogr.2023.04.001

Naqa, I. E., & Murphy, M. J. (2015). Machine learning in radiation oncology. Nature Reviews Clinical Oncology, 12(12), 747–756.

Nasir Mustafa (2023) Automating Threat Intelligence Ingestion and Analysis DOI:10.13140/RG.2.2.33608.39680

Noura Alshathry, Alex-Stefan Carare, Snehith Galiveeti, Rishit Garg and Dhyey Mehta | Jul 27, 2024 | Computer Science | 0 Machine Learning Algorithms for Detecting and Preventing Cyber Threats

Ocha (2024) Rapid response Mechanism Humanitarian Response Plan

Oltsik, J. (2019). Cyber threat intelligence: A framework for success. CSO.

Olumachukwu Chialaka (2024) The Importance of Cybersecurity in the Digital Age

Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2016). Practical black-box attacks against deep learning systems using adversarial examples.

Perlman, A. (n.d.). How Machine Learning Enhances Cybersecurity. Retrieved from (link unavailable)

Petar Radanliev (2018) Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0 DOI:10.1049/cp.2018.0041

Prague, Czech Republic Et al (2020), The History of Cybercrime And Cybersecurity, 1940-2020

Rachid Ejjami Et al (2024) Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives DOI:10.70792/jngr5.0.v1i1.5

Ritish Verma (2024) Cybersecurity Challenges in The Era of Digital TransformationDOI:10.25215/9392917848.20

Rohith Vallahaneni Et al (2024) Utilizing AI and Machine Learning in Cybersecurity for Sustainable Development through Enhanced Threat Detection and Mitigation

Russell, S. J., & Norvig, P. (2010). Artificial intelligence: A modern approach. Prentice Hall.

Russell, S. J., & Norvig, P. (2010). Artificial intelligence: A modern approach. Prentice Hall.

Russell, S. J., & Norvig, P. (2010). Artificial intelligence: A modern approach. Prentice Hall.

Sarker, I. H., et al. (2020). Machine learning and cybersecurity: A review. Journal of Intelligent Information Systems, 57(2), 277-293.

Sarker, I. H., et al. (2020). Machine learning and cybersecurity: A review. Journal of Intelligent Information Systems, 57(2), 277-293.

Sharp, R. (2007). An Introduction to Malware.

SHASHID ALARM 2022 Cybersecurity: Past, Present and Future

Shoumya Singh[1] and Deepak Kumar[2(2024)]

Singh, R., et al. (2020). AI-powered cybersecurity: A survey. Journal of Cybersecurity, 6(1), 1-12.

Singh, R., et al. (2020). Malware detection and analysis: A survey. Journal of Intelligent Information Systems, 57(2), 297-313.

Strategies Hider Ali (2024) Advanced Persistent Threats (APTs): Analysis, Detection, and Mitigation

UPES (2024) Cybersecurity in the Digital Age

World Economic Forum. (2020). Global risks report 2020.

World Economic Forum. (2020). Global risks report 2020.

Zamfiroiu Alin (2022) Cybersecurity Management for Incident Response DOI:10.54851/v4i1y202208