International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)

ISSN: 2456-236X

Vol. 10 Issue 01 | 2025

Artificial Intelligence in Cybersecurity: Enhancing Intrusion Detection System

Sangeeta Singh1, Dr.Manjiri U. Karande[2]

[1]Assistant Professor, Department of Computer Science Engineering, Madhav University, Pindwara, Rajasthan

[2]Assistant Professor, Department of Computer Science & Engineering, Padm. Dr. V. B. Kolte College of Engineering, Malkapur, Maharashtra, India

DOI: **10.5281/zenodo.15751566**

ABSTRACT

With the growing complexity and scale of cyber threats, traditional security mechanisms are no longer sufficient to protect digital infrastructures. Artificial Intelligence (AI), particularly Machine Learning (ML), has emerged as a transformative force in enhancing cybersecurity, especially in the area of Intrusion Detection Systems (IDS). The study highlights the role of AI in both protecting and attacking security systems, and identifies the key areas where AI significantly contributes to cybersecurity, such as anomaly detection, behavioral analysis, and predictive threat modeling. We explore various AI methodologies, their applicability in threat modeling, and the role of AI as both a defensive and adversarial tool. In addition to presenting a comprehensive review of existing literature, this study identifies significant research gaps and highlights the advantages and limitations of current IDS approaches. Our contributions also include a structured overview of cybersecurity software tools and AI-driven frameworks, aiming to offer future-ready solutions for cyber threat intelligence. It further outlines the scope, contributions, and research gaps in AI-driven cybersecurity frameworks, presenting the advantages and limitations of current IDS technologies, especially in detecting zero-day attacks and supporting real-time threat mitigation. This work underscores the need for robust, adaptive, and transparent AI systems to advance the security posture of modern networks.

Keywords: ***Cyber Security, Cyber Attacks, IDS, Artificial Intelligence, , Network Security, Machine Learning Internet of Things (IoT) Security, Cyber Security Frameworks, Malware.***

1. INTRODUCTION

The growing global digitization of processes has increased the activity of cybercriminals, who aim to obtain financial and personal advantages by breaking into people's and organizations private information. Consequently, there are serious risks to information systems, which must be highly protected in order to thwart any malevolent attack. As a result, cybersecurity professionals are also striving to constantly improve security protocols and standards that can protect individuals and institutions from data or financial loss. One of the most crucial topics for IT professionals to research and practice is cyber security. Cyber security, according to Jang-Jaccard[4], is the set of practices and guidelines used to defend computers, databases, servers, and networks against online threats such as malware, theft, and attacks. Every company is trying to make sure they have the best cybersecurity.

According to J. Jang -Jaccard, cybersecurity is defined as the procedures and policies adopted to protect the computers, databases, servers, and networks from the cyber threats like attacks, thefts, malware, etc. The Cybersecurity is continually evolving due to the fast-paced nature of research. The cybersecurity community acknowledges that it is impossible to completely eradicate cyber threats. A cyber attack involves one or more computers targeting another computer with the intent to disable it, take its services offline, or access its data. To address these challenges, many organizations are increasingly using artificial intelligence (AI) tools to combat cyber threats. AI has enabled organizations to enhance their security measures and lower the risk of breaches. Machine learning and AI are crucial technologies in information security, assisting companies and individuals in identifying and analyzing potential threats to their operations.

Therefore research and technological advancement are crucial to reduce the negative effects of cyber attacks. Cyberattacks seek to compromise the confidentiality, integrity, and availability of linked services, resources or systems by gaining access to them. In order to avoid or mitigate security issues before they cause harm in cyberspace, research has looked for a more proactive strategy. Intelligent cyber defense techniques must be created to handle the variety and dynamics of threats in order to raise the degree of cyber security. AI offers data to monitor every step of the production process. It enables better management to adjust output levels based on demand, with the goal of minimizing downtime to maintain system efficiency. The concepts of confidentiality, integrity and availability (CIA) as they relate to cyber security are depicted graphically in Figure1

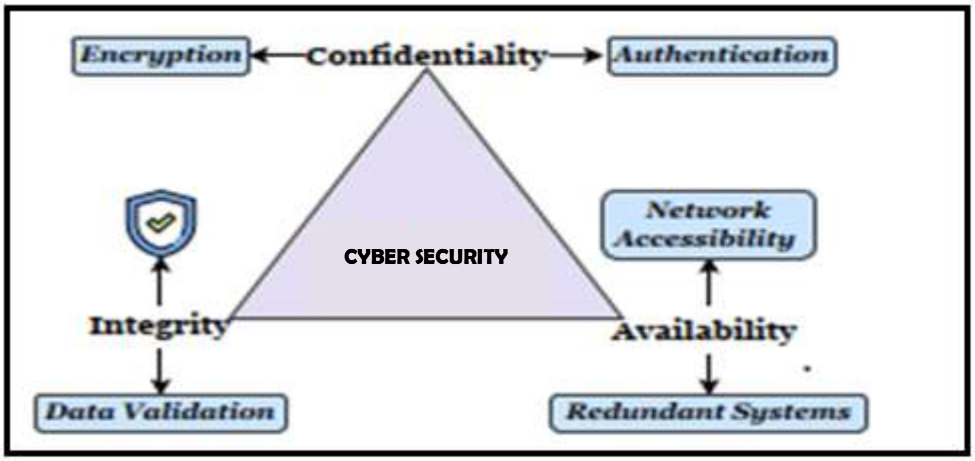

Fig. - 1. Triangle of confidentiality, integrity and availability for data security

2. OBJECTIVE OF CYBERSECURITY

The objective of cybersecurity is to ensure the availability, integrity, confidentiality, and no repudiation of information and information management systems through various cyber defence techniques [27] [Li, Jie, et al., This ensures that information such as medical records, financial records, and personal identity are protected from malicious attacks.

- **Confidentiality**: This rule underscores the significance of avoiding unauthorized information get to. Maintaining Confidentiality is vital to preempt potential misappropriation or misuse of delicate data, which, in case misused, seem compromise the secure and dependable operation of cyber security frameworks.
- **Integrity**: Integrity depends on the authenticity, precision, and consistency of data throughout their entire life cycle. It includes not only the identification of unauthorized data access but also the prevention of unauthorized data modification. Safeguarding data integrity is essential for maintaining the reliability of a system and its ability to make decisions.
- **Availability**:A system's adequacy is based on the dependable availability of its functions and its ability to work as expected. In the context of cyber security, any loss of accessibility can lead to immediate and severe security concerns. The complexity in security is important, emphasizing its key aspects due to its straightforward nature and little need for adjusting settings. Such methods offer promising alternatives to traditional AI models.
- **No repudiation:** Ensuring that information cannot be denied by the sender or system when it is already transmitted

3. CYBER SECURITY FRAMEWORK

A cyber security framework consists of a collection of documents that portray an organization's optimal practices for managing cyber security threats. These systems effective reduce a organizations exposure to vulnerabilities. The Cyber Security Framework (CSF) serves as a set of guidelines that private sector companies can utilize to detect, identify, and respond to cyber threats. This model is adopted globally, including voluntary implementation by banks, energy companies, defense contractors, and telecommunications firms. These represent the five primary functions of the cyber security framework. This framework will provide outline r how to actualize a five-step approach to cyber security.

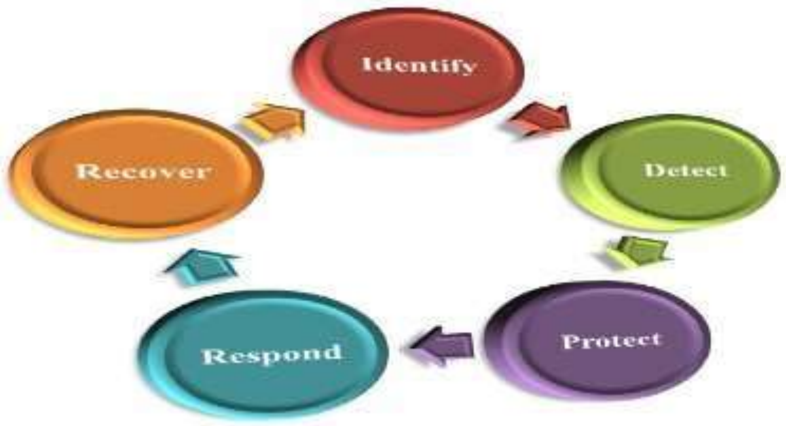

Fig. 2: Function of Cyber Security Framework

- **Identify**: To effectively handle threats to cybersecurity regarding systems, assets, information, and capabilities, organizations must first comprehend their environment.
- **Detect**: Institutions should establish the appropriate procedures to promptly detect cybersecurity events.
- **Protect**: Institutions need to create and execute effective measures to minimize or manage the repercussions of potential cybersecurity incidents.
- **Respond**: Institutions must be prepared to develop strategies to plan the consequences of cyber intrusions.
- **Recover**: Institutions should design and implement robust strategies to recover systems or services impacted by cybersecurity events.

The cybersecurity framework is beneficial at every phase of software development. This framework is intended to be adaptable.

4. LITERATURE REVIEW

According to the “2021 SonicWall Cyber Threat Report,” there was a 62% increase in global ransomware attacks in 2020, with over 304 million ransom ware attacks reported. The need for more effective cybersecurity measures has never been greater, driving the development of innovative techniques such as Artificial Intelligence (AI) and Machine Learning (ML) algorithms (Alsheikh et al., 2021).

Malware attacks make up the majority of cyber attacks, accounting for 43% of the total, with 5.6 billion attacks (Sharma et al., 2022). Intrusion attempts are the second most common type of attack, counting for 20% of the total, with 4.8 trillion attempts (Katz et al., 2019).

Ransomware attacks are also a significant threat, accounting for 62% of the total, with 304.6 million ttacks. Cryptojacking attacks, although relatively less frequent, still constitute a considerable threat,
accounting for 28% of the total, with 304.6 million attacks. Encrypted threats, on the other hand, are much less common, accounting for 4% of the total, with only 3.8 million attacks. IoT attacks are also comparatively rare, accounting for 66% of the total, with 56.9 million attacks (Feeken et al., 2022).

The author in [Li, J.H. 5] discussed the intersection of AI and cybersecurity. More particularly, the paper reviewed some ML and DL approaches to counter against cyber attacks. What is more, the author introduced the possibility of attacking the AI model. Nevertheless, the paper just discussed adversarial attacks and ignored other kinds of attack using the AI model, such as poisoning data, and the extraction model.

A recent study conducted by [Faris et al. 8] presented an email spam detection and identification system based on a genetic algorithm (GA) and a random weight network (RWN). According to the experiments, the proposed system obtained remarkable results in terms of accuracy, precision, and recall.

Table -1 Shows all areas of AI for IDS in cyber security applications

Application Area	Description of AI/ML Algorithms Uses
Network Security	Supervised and Unsupervised learning methods, such as neural networks, Random Forest and SVM, are used to detect network-based attacks and intrusions
Malware Detection	Unsupervised learning methods, such as Clustering and anomaly detection, are used to group similar malware together and detect new and unknown malware.
Security Automation	Rule-based and Machine learning techniques are used to automate repetitive and time-consuming tasks such as vulnerability scanning, patch management and incident response.
Threat Intelligence	Unsupervised learning methods, such as Clustering, are used to group similar threats together and identify new and emerging threats.
Security Management	AI-based systems can be used to improve security operations, incident response and incident management, through automation and incident analysis.
Anomaly Detection	Unsupervised learning methods, such as density- based clustering and one-class SVM, are used to detect unusual or malicious activities in the network or system.
Intrusion Detection and Response	Supervised learning methods, such as Random Forest, SVM and neural networks are used to classify network connections as normal or anomalous.
Vulnerability Management	AI-based systems can use techniques such as rule- based systems, decision trees and clustering to scan systems and networks to identify potential vulnerabilities and prioritize them based on the level of risk they pose.
Security Education and Awareness	AI and ML can be used to create personalized and interactive security training content that is tailored to the specific needs and knowledge level of the individual, and also by using gasification and AI based chat bots to provide real-time support and guidance.
Cyber-attack Predriction	Supervised learning methods, such as Random Forest, SVM and neural networks, are used to predict cyber attacks by identifying patterns and anomalies in network traffic and behavior.

5. SCOPE OF THE RESEARCH AND KEY CONTRIBUTIONS

This research focuses on narrowing the gap between the real-world needs of cybersecurity and the growing capabilities of Machine Learning (ML) and Deep Learning (DL). By doing so, we aim to offer solutions to today’s pressing security challenges.

The key contributions of our work are:

- ➢ We explore how artificial intelligence (AI) plays a vital role in strengthening cybersecurity.
- ➢ We provide a detailed and organized classification of existing cybersecurity frameworks.
- ➢ We explain how AI is used in Intrusion Detection Systems (IDS) for cybersecurity applications.
- ➢ We outline the AI-based methodologies adopted in our study for cybersecurity solutions.
- ➢ We examine how AI and ML are applied specifically in IDS techniques.
- ➢ We review various software tools used for ensuring cybersecurity.
- ➢ We highlight existing research gaps in the field of AI-powered cybersecurity.
- ➢ We discuss how AI can be used to develop future-focused solutions for cyber threat intelligence.

- We present a comprehensive review of the current challenges in applying AI to cybersecurity and areas that still need further research.
- We also look at the obstacles and future research directions for machine learning in this field.

6. ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

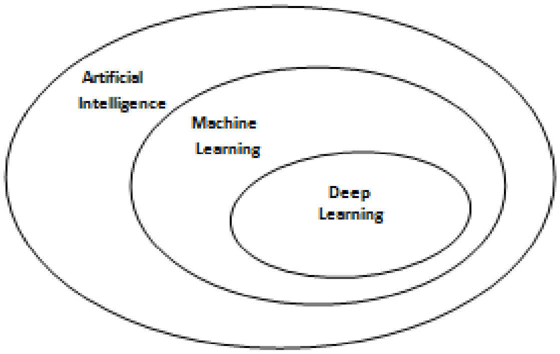

Fig. 3 Relationship between AI, ML, and DL

AI has the potential to automatically provide significant cyber security insights without human interaction. The goal of AI is to endow machines with human intelligence. Machine learning is a method to implement AI using algorithms to analyze and learn from data. Deep learning is a technology used in the process of machine learning, enabling the expansion of the scope of AI . The essence of AI is based on the context that human intelligence can be accurately described, enabling its replication by machines and/or software. In the following sections, we provide an overview of the most promising tool for attacking AI model in cybersecurity.

AI as a Tool for Attacking AI Models

AI tools are advanced software systems that use artificial intelligence to perform tasks smartly and efficiently. They can analyze large data sets, recognize patterns, and even learn from experience. These tools are widely used in fields like healthcare, cybersecurity, finance, and education, Examples include virtual assistants, chatbots, and image recognition software. Overall, AI tools help save time, reduce human error, and improve decision-making. Adversarial input attacks, poisoning attacks, and model extraction attacks are significant threats in the field of artificial intelligence and machine learning. These attacks target the integrity, reliability, and confidentiality of AI systems, posing challenges to their safe deployment.

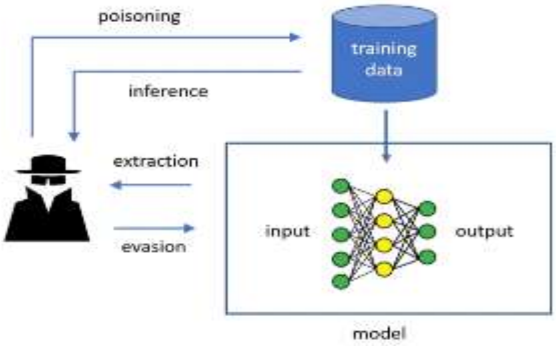

Fig. 4 Adversarial Attacks Model

Adversarial input attacks - It involve making small, often imperceptible changes to input data like images or text which can cause AI models to make incorrect decisions. These attacks exploit vulnerabilities in the model's decision boundaries, making them dangerous in applications like autonomous driving, facial recognition, and medical diagnosis.

Poisoning attacks – It occurs during the training phase of machine learning. In these attacks, an adversary injects malicious or misleading data into the training dataset. As a result, the model learns flawed patterns, leading to unreliable or biased outcomes. This type of attack can silently degrade model performance and is particularly dangerous in systems trained on crowd sourced or open datasets. Poisoning can also be targeted, aiming to misclassify specific inputs while the rest of the model behaves normally, making detection harder.

Model extraction attacks – It involve an attacker attempting to steal a machine learning model by querying it repeatedly and analyzing its outputs. Over time, the attacker can approximate the structure, parameters, or behavior of the original model. This not only compromises intellectual property but also exposes the model to further attacks like adversarial inputs. These extraction techniques threaten the commercial and security value of proprietary models deployed through APIs.

7. AI METHODOLOGY FOR CYBERSECURITY

By offering intelligent, adaptive, and real-time threat detection capabilities, intrusion detection systems (IDS) powered by artificial intelligence (AI) are transforming cyber security. In contrast to AI models, particularly those based on machine learning and deep learning, which are more accurate at analyzing complex patterns, detecting anomalies, and identifying emerging threats, traditional IDS frequently have trouble managing massive volumes of data or identifying novel threats. By continuously learning from fresh data, these systems are able to adjust to changing attack tactics like advanced persistent threats (APTs), insider threats, and zero-day exploits. AI-powered intrusion detection systems can also improve network performance and security posture by reducing false positives by distinguishing between malicious and legitimate activity. AI-powered IDS can lower false positives, enhancing network performance and security posture overall. Businesses can significantly improve their defenses by combining AI with IDS to create proactive defenses that not only recognize threats but also react to them instantly.

Learning Algorithms

Generally, learning algorithms help to enhance performance in accomplishing a task through learning and training from experience. There are currently three major types of learning algorithms which we use to train machines. This section is an overview of the learning algorithms, an essential concept of AI. Furthermore, we present a brief information related to opportunities and challenges about ML algorithms, DL algorithms, and their computation methods that are frequently utilized in the area of cybersecurity.

Table -2 Learning algorithms importance and challenges

Learning algorithms	Opportunities	Challenges
Machine learning algorithms	Can analyze vast amounts of data to identify patterns and predict potential threats.	Requires a large amount of data to effectively train the model.
Deep learning algorithms	Can identify previously unknown threats and adapt to changing attack patterns.	Requires significant computational resources to effectively train the model.
Supervised Learning	High accuracy in detecting known threats	Requires labeled training data.
Unsupervised machine learning	Capable of identifying patterns or behaviors that deviate from the normal or expected behavior of a system without the need for labeled data	May produce a large number of false positives or false negatives
Reinforcement learning (RL)	Able to learn from previous experiences and make decisions based on the current situation, enabling adaptive and efficient responses to new and unknown threats	Need significant computational resources and expertise to implement
Deep neural networks (DNN)	Able to analyze network traffic and detect anomalies that may indicate an attack, such as unusual data transmission patterns or attempts to access restricted resources	Require massive amounts of data to effectively train the model

Generative models (e.g. GANs, VAEs)	Can generate synthetic data for training and improve detection	Limited interpretability and explain ability

8. AI / ML INTO INTRUSION DETECTION TECHNIQUES (IDS)

Intrusion detection systems (IDS) frequently employ hybrid models that combine signature-based techniques—effective at quickly identifying known threats with minimal false alarms with anomaly based techniques that detect unusual behaviors. An evolving trend is the integration of AI with other computational intelligence methods such as Ant Colony Optimization and Particle Swarm Optimization, further enhancing detection capabilities.

Table -3 IDS Advantage and Limitation

AI/ML Intrusion Detection Techniques	Advantages	Limitation
Anomaly Detection	Effective for identifying unknown threats	Difficult to differentiate between benign and malicious anomalies
Zero-day attack detection	Can identify and block previously unknown threats.	May be less effective against complex or targeted attacks.
Behavioral detection technology	Learns normal network behavior to identify and classify anomalies, can identify potential cyber- attacks	May generate false positives or false negatives, leading to unnecessary alerts or missed threats.
Predictive threat modeling	Can analyze large amounts of data to identify emerging threats and potential attack vectors.	Requires accurate data inputs and ongoing updates to remain effective.
Personalized machine learning models	Can provide tailored protection based on user behavior and preferences.	May require significant processing power and storage capacity.
Real-time monitoring and analysis	Can detect and respond to threats as they occur.	Requires significant resources and can generate a high volume of alerts.

RESEARCH GAPS IN AI-BASED CYBERSECURITY

Our study has highlighted several key areas where further research is needed. While this list is not complete, it includes some of the **biggest challenges:**

- **Building effective AI models** with little data, changing the focus from large amounts of data to maximizing small data situations.
- **Creating complete solutions** that can work straight with raw data, cutting down or removing the need for complicated feature design ordeep knowledge of the field.
- **Adding change detection and flexibility** into models so they can manage changing data patterns and system behaviors over time.
- **Regularly checking AI models** to find and fix biases early, which could otherwise lead to new security problems.
- **Discovering ways to remove existing biases** or data imbalances that can influence the model's performance and trustworthiness.
- **Creating standardized datasets** that follow clear rules, so researchers can accurately test, reproduce, and compare different AI-based cybersecurity solutions.

9. SECURITY TOOLS FOR CYBER SECURITY

In today's world, no organization can successfully reduce cyber threats and security problems without strong cyber security team. Cybercriminals are always looking for weaknesses to take advantage of putting businesses at risk. India ranks third among the top ten countries most targeted by cyber attackers. Cyber security software is crucial for safeguarding sensitive and private information held by both businesses and individuals. Table 1 gives an overview of the main types of cyber security software tools discussed in this section.

Table-4 Type of Software Tools in Cyber Security

Software	Our Ratings	Best For	Category	Features
LifeLock	5 Stars	Small to large businesses.	Identity theft protection	Block cyber threats, detect & alert, restore & reimburse
Cyber control	5 Stars	Small to medium size businesses.	Vulnerability scanning	Fraud detection reporting suite and file security for data privacy and GDPR
Intruder	5 Stars	Small to large businesses.	Cloud based vulnerability scanner	Check for web application flaws, emerging threats notifications, PCI ASV scan available
Indeni	4.5 Stars	Small to large businesses.	Behavioral Analytics incident Management	Incident is an automated crowd-sourced cybersecurity platform for network and security infrastructure
Malware bytes	4.5 starts	Small to large businesses and personal use	Cybersecurity for home and business	Multilayer protection, prevention of threats in real times etc.
Mimecast	5 Stars	Small to large businesses.	Email security and compliance platform	Cyber resilience for Email, Email Security web security cyber security training etc
Site lock	5 Stars	Small to medium size businesses.	Website security	Enhances security testing for the websites and accelerates the performance, two factor authentication web threats management
Solar Wind Security Event Manager	5 Stars	Small to large businesses.	Cloud based tool for SIEM	Threat intelligence, SIEM Security & Monitoring Log correlation & Analysis, Network & Host Intrusion Detection, etc
Bit defender	5 Stars	Small to large businesses	Cyber security software	Multilayer ransom ware Protection, Network threat protection etc
Webroot	4.5 starts	Business to home use	Cyber security for endpoints networks , PC and mobile devices	Predictive threat intelligence, Multi vector protection, Real time protection
Snort	5 Stars	Small to medium size businesses.	Network intrusion prevention system	Real time packet analysis, packet logging
wire shark	5 Stars	Public and private organization body, educational institutions	Network protocol analyzer	Decryption of various protocols , output in XML postscript , CSV or plain text
CIS	5 Stars	Small to large businesses.	Cyber security Tools	Securing a specific platform and tracking specific threats, security organization

10. AI FOR FUTURE SOLUTIONS IN CYBER THREAT INTELLIGENCE

Artificial Intelligence (AI) is rapidly becoming a cornerstone of cyber threat intelligence (CTI), enabling organizations to predict, detect, and respond to threats more efficiently and effectively. As cyber-attacks grow in sophistication and scale, Artificial Intelligence (AI) is transforming the future of system by providing intelligent, efficient, and secure solutions to various challenges in the system. As cyber security becomes more integrated into modern system, AI offers several key benefits that enhance both the functionality and trustworthiness of these systems.

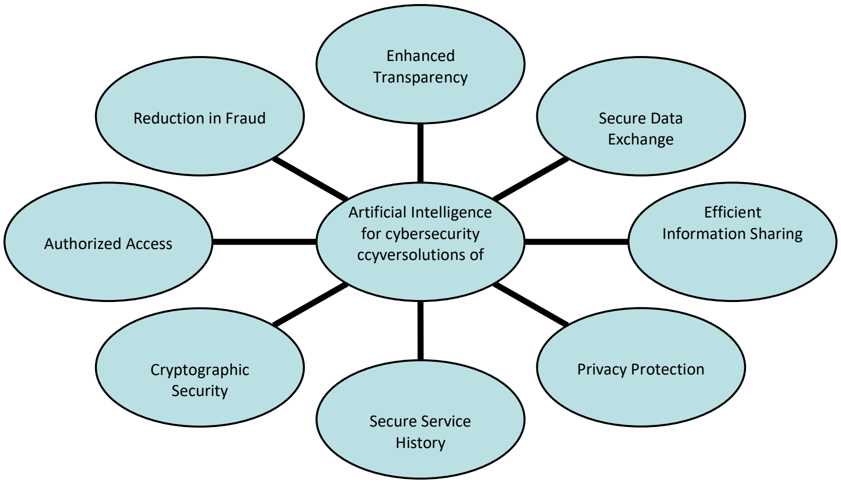

Fig - 6. **Artificial Intelligence for cyber security**

i. **Tracking Location of Threat Actors**

AI-powered threat intelligence tools can trace the origin of cyber attacks by analyzing metadata, IP logs, device signatures, and behavioral patterns. This capability helps organizations pinpoint attackers geographically or organizationally, allowing for quicker response and potential legal action.

ii. **Enhanced Transparency**

AI brings clarity and visibility into complex cyber environments. AI improves transparency across networks by providing continuous monitoring, real-time alerting, and automated reporting, AI enhances transparency across networks and endpoints, allowing security teams to gain deeper insight into ongoing threats and vulnerabilities.

iii. **Reduction in Fraud**

AI can detect fraudulent behaviors by analyzing massive amounts of transaction and activity data in real-time. Whether it's phishing attempts, impersonation, or financial fraud, AI systems recognize abnormal patterns and trigger alerts, preventing damage before it escalates.

iv. **Secure Data Storage and Processing**

AI helps protect CTI data through intelligent encryption, classification of sensitive information, and real-time risk assessment. It identifies potential weaknesses in data handling processes and prevents unauthorized access or data leakage.

v. **Authorized Access and Identity Verification**

AI enhances advanced identity and access management (IAM) systems by continuously verifying user behavior, detecting anomalies, and ensuring that only authorized individual can access sensitive threat intelligence systems and data.

vi. **Privacy Protection in Data Exchange**

In the CTI ecosystem, data must often be shared across agencies and organizations. AI enables secure data exchange by ensuring compliance with privacy regulations, anonymizing personally identifiable information (PII), and enforcing access controls to protect data integrity.

vii. **Security of Sensitive Intelligence**

AI actively monitors and protects critical CTI assets such as threat databases, intelligence feeds, and vulnerability reports. It uses behavior analytics to identify unauthorized access or tampering and ensures that sensitive intelligence remains secure.

viii. **Cryptographic Security Enhancement**

AI improves cryptographic systems by dynamically managing encryption keys, predicting and mitigating cryptographic vulnerabilities, and optimizing encryption protocols based on threat levels. This provides robust protection for both stored and in-transit data.

ix. **Security for Sensitive Intelligence.**

AI actively monitors and safeguards vital CTI assets, including as threat databases, intelligence streams, and vulnerability assessments. It employs behavior analytics to detect illegal access or tampering and keeps sensitive intelligence secure.

x. **Secure Threat and Response History**

It is crucial to maintain a secure, tamper-proof record of previous cyber incidents for the purposes of learning and legal compliance. AI can automatically log, encrypt, and store cyber events, facilitating thorough forensic analysis and effective strategy modifications for future threats.

Artificial Intelligence is revolutionizing cyber threat intelligence by enabling faster, smarter, and more proactive responses to threats. From real-time fraud detection to secure data handling and privacy protection, AI ensures that organizations stay resilient in an ever-evolving digital threat landscape.

11. CHALLENGES AND OPEN RESEARCH DIRECTIONS

Artificial Intelligence (AI) is increasingly contributing to the enhancement of cybersecurity and shows significant potential for the future. Nevertheless, effectively utilizing AI in this domain presents several substantial challenges. A primary concern is the precision and dependability of AI systems. If an AI model generates an excessive number of false positives, it can result in an overwhelming number of unnecessary alerts, thereby squandering time and resources. Conversely, if it fails to identify genuine threats (false negatives), it may leave systems exposed to severe cyberattacks.

Another significant obstacle is the requirement for extensive amounts of high-quality data. Numerous existing AI-driven tools necessitate substantial training data to function optimally. However, in practical scenarios, acquiring such data for cybersecurity applications proves to be challenging. Issues related to privacy, variations in data formats across different systems, and the complexities of data labeling all contribute to the difficulties in collecting the necessary information.

Furthermore, AI in cybersecurity must contend with intelligent and continuously evolving adversaries. Attacks aimed at deceiving AI systems—known as adversarial attacks—are becoming increasingly prevalent and more difficult to thwart. This results in an ongoing arms race between cyber defenders and attackers. Regrettably, AI can be leveraged by both parties. While it aids in safeguarding against threats, it can also be exploited by cybercriminals to develop more sophisticated and elusive attacks that are challenging to detect using conventional tools.

Open Research Directions

As artificial intelligence increasingly integrates into cybersecurity, malicious actors are also adapting their strategies to exploit it. This phenomenon is referred to as adversarial machine learning, wherein cybercriminals attempt to deceive or compromise AI systems. Typically, these attacks manifest in three primary forms: providing erroneous input to AI, tampering with its training data (known as poisoning), or appropriating the model.

Poisoning attacks pose a particularly significant threat. They entail the introduction of harmful data during the training phase, which can diminish the AI's capability to detect threats effectively. Such attacks have already been observed in domains such as spam detection and malware analysis. Recent research indicates that AI may be integrated with swarm-like communication, akin to the collaborative behavior of insects or drones. This integration could facilitate the development of sophisticated, stealthy malware capable of spreading discreetly and persisting even amidst network disruptions. Consequently, this could result in more severe threats, including advanced worms, Trojans, or ransomware. In light of these developments, continuous research is crucial. It is imperative to enhance

AI tools to ensure they are more secure, adaptable, and intelligent, while simultaneously acknowledging the inherent risks they present.

Through our study, we've identified several important areas where future research is still needed. While this isn't an exhaustive list, it highlights some of the most pressing challenges:

- Training AI with Limited Data: Many current models rely on huge datasets, but real-world cybersecurity often lacks this. Future research needs to focus on building effective AI systems that can still perform well with limited or small amounts of data.
- Working Directly with Raw Data: There's a need to develop end-to-end solutions that can handle raw data without requiring complex feature engineering or deep domain expertise.
- Adapting to Change: AI models should be able to detect changes and adapt to evolving patterns in data and system behavior over time—something many existing systems struggle with.
- Addressing Bias Early: Regular monitoring of AI models is essential to spot and correct biases before they become serious security issues.
- Handling Data Imbalance: Research is needed on how to eliminate existing biases or imbalances in datasets, which can negatively affect a model's accuracy and reliability.
- Standardizing Datasets: There's a lack of universally accepted, high-quality datasets. Creating benchmark datasets with clear rules will help researchers fairly test, replicate, and compare different AI-based cybersecurity approaches.

12. CONCLUSION

The growing use of Artificial Intelligence in cybersecurity marks a significant step forward in tackling today's increasingly complex cyber threats. As AI becomes more deeply embedded in cybersecurity, it's clear that its vulnerabilities are being actively explored and exploited by attackers. From poisoning training data to developing stealthy malware using swarm intelligence, the risks are evolving alongside the technology. In this study, we explored how AI and Machine Learning are being integrated into Intrusion Detection Systems to improve how we detect, understand, and respond to security incidents. While AI provides substantial benefits—such as anomaly detection, real-time monitoring, and adaptive learning models—it also introduces challenges, including adversarial inputs, lack of interpretability, and model vulnerabilities. Our review of the literature and tools shows a growing but still maturing field, where opportunities for innovation remain vast. Addressing current research gaps, especially in zero-day detection and model transparency, will be key to building next-generation IDS solutions. These technologies offer powerful capabilities—like spotting unusual behavior, analyzing threats in real time, and adapting to new attack patterns. However, they also bring new challenges, such as dealing with misleading inputs, understanding how decisions are made, and addressing weaknesses in the models themselves. This study illustrated both the strengths and limitations of AI-driven computation methods in cyber security and highlighted uses of various AI/ML learning algorithm in intrusion detection system. By comparing our findings with existing research related to software security tools for cyber security (refer to Table 4), we aimed to provide a useful and important perspective. Moving forward, continuous research is critical to building AI systems that are not only smarter but also more resilient—capable of withstanding emerging threats in an ever-changing digital world.

REFERENCE

[1] S. Dua and X. Du, Data mining and machine learning in cybersecurity. CRC press, 2016.

[2] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," Computers in Human Behavior, vol. 48, pp. 51-61, 2015. https://doi.org/10.1016/j.chb.2015. 01.039

[3] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 5, no. 80, pp. 973-993, 2014. https://doi.org/10.1016/ j.jcss.2014.02.005

[4] Jang-Jaccard, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences Volume 80, Issue 5, August 2014, Pages 973-993, https://doi.org/10.1016/j.jcss.2014.02.005

[5] Li, J.H. Cyber security meets artificial intelligence: A survey. Front. Inf. Technol. Electron. Eng. 2018, 19, 1462–1474. [CrossRef]

[6] M. P. Johnston, "Secondary data analysis: A method of which the time has come," Qualita- tive and quantitative methods in libraries, vol. 3, no. 3, pp. 619-626, 2017.

[7] M. Akbari Roumani, C. C. Fung, S. Rai, and H. Xie, "Value analysis of cyber security based on attack types, " ITMSOC: Transactions on Innovation and Business Engineering, vol. 1, pp. 34-39, 2016.

[8] Faris, H.; Ala'M, A.Z.; Heidari, A.A.; Aljarah, I.; Mafarja, M.; Hassonah, M.A.; Fujita, H. An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks. Inf. Fusion 2019, 48, 67–83. [CrossRef]

[9] Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. Network anomaly detection: A machine learning perspective. Chapman and Hall/CRC, 2019.

[10] Berman, Daniel S., et al. "A survey of deep learning methods for cybersecurity." Information 10.4 (2019): 122. https://doi.org/10.3390/info10040122.

[11] Depren, Ozgur, et al. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." Expert systems with Applications 29.4 (2005): 713-722. https://doi.org/10.1016/j.eswa.2005.05.002. Accessed 25.07.2021.

[12] Sarker, Iqbal H., et al. "Cybersecurity data science: an overview from machine learning perspective." Journal of Big data 7.1 (2020): 1-29. https://doi.org/10.1186/s40537-020-00318-5.

[13] Thomas, Tony, Athira P. Vijayaraghavan, and Sabu Emmanuel. Machine learning approaches in cybersecurity analytics. Springer, 2020, https://doi.org/10.1007/978- 981-15-1706-8.

[14] Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Comput. Ind. 2020, 114, 103165. [CrossRef]

[15] Alsheikh, M., Konieczny, L., Prater, M., Smith, G., & Uludag, S. (2021). The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. IEEE Consumer Electronics Magazine, 11 (3), 59–68.

[16] Feeken, L., Kern, E., Szanto, A., Winnicki, A., Kao, C. Y., Wudka, B. Burghardt, C. (2022). Detecting and Processing anomalies in a factory of the future. Applied Sciences, 12(16), 8181. https://doi.org/10. 3390/app12168181

[17] Katz, M., Pirinen, P., &Posti, H. (2019, August). Towards 6G: Getting ready for the next decade. Proceedings of the 2019 16th International symposium on wireless communication systems (ISWCS), Oulu, Finland (pp. 714–718). IEEE.

[18] Kaloudi, N.; Jingyue, L.I. The AI-based cyber threat landscape: A survey. ACM Comput. Surv. 2020, 53, 20. [CrossRef]

[19] Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A survey of deep learning methods for cyber security. Information 2019, 10, 122. [CrossRef]

[20] Barton, M.; Budjac, R.; Tanuska, P.; Gaspar, G.; Schreiber, P. Identification Overview of Industry 4.0 Essential Attributes and Resource-Limited Embedded Artificial-Intelligence-of-Things Devices for Small and Medium-Sized Enterprises. Appl. Sci. 2022, 12, 5672. [CrossRef]

[21] A.; Karras, A.; Theodorakopoulos, L.; arras, C.; Kranias, P.; Schizas, N.; Kalogeratos, : Sophisticated Attacks, Safety Issues, G.; Tsolis, D. Autonomous Vehicles Challenges, Open Topics, Blockchain, and Future Directions. J. Cybersecur. Priv. 2023, 3, 493–543. https:// doi.or g/10.3390/jcp3030025 Chang, V.; Doan, L.M.T.; Di Stefano, A.; Sun, Z.; Fortino, G. Digital payment fraud detection methods in digital ages and Industry 4.0. Comput. Electr. Eng. 2022, 100, 107734. [CrossRef]

[22] Elsisi, M.; Tran, M.Q.; Mahmoud, K.; Mansour, D.E.A.; Lehtonen, M.; Darwish, M.M.F. Towards Secured Online Monitoring for Digitalized GIS against Cyber-Attacks Based on IoT and Machine Learning. IEEE Access 2021, 9, 78415–78427. [CrossRef]

[23] Le, D.D.; Pham, V.; Nguyen, H.N.; Dang, T. Visualization and explainable machine learning for efficient manufacturing and system operations. Smart Sustain. Manuf. Syst. 2019, 3, 127–147. [CrossRef]

[24] Mendonça, R.V.; Silva, J.C.; Rosa, R.L.; Saadi, M.; Rodriguez, D.Z.; Farouk, A. A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. Expert Syst. 2022, 39, e12917. [CrossRef]

[25] Tran, M.Q.; Elsisi, M.; Mahmoud, K.; Liu, M.K.; Lehtonen, M.; Darwish, M.M.F. Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment. IEEE Access 2021, 9, 115429–115441. [CrossRef]

[26] Yang, H.; Zhan, K.; Kadoch, M.; Liang, Y.; Cheriet, M. BLCS: Brain-Like Distributed Control Security in Cyber Physical Systems. IEEE Netw. 2020, 34, 8–15. [CrossRef]

[27] M. Wazid, A.K. Das, V. Chamola et al. Uniting cyber security and machine learning: Advantages, challenges and future research, ICT Express 8 (2022), Pg. No-313–321

[28] Trung, N.D.; Huy, D.T.N.; Huong, L.T.T.; Van Thanh, T.; Thanh, N.T.P.; Dung, N.T. Digital Transformation, AI Applications and IoTs in Blockchain Managing Commerce Secrets: And Cybersecurity Risk Solutions in the Era of Industry 4.0 and Further. Webology 2021, 18, 453–465. [CrossRef]

[29] Laghari, S.U.A.; Manickam, S.; Al-Ani, A.K.; Rehman, S.U.; Karuppayah, S. SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape. IEEE Access 2021, 9, 154380–154394. [CrossRef]

[30] Alohali, M.A.; Al-Wesabi, F.N.; Hilal, A.M.; Goel, S.; Gupta, D.; Khanna, A. Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. Cogn. Neurodyn. 2022, 16, 1045–1057. [CrossRef]

[31] Mubarakova, S.R.; Amanzholova, S.T.; Uskenbayeva, R.K. Using Machine Learning Methods in Cybersecurity. Eurasian J. Math. Comput. Appl. 2022, 10, 69–78. [CrossRef]

[32] Li, Jie, et al. "Machine learning algorithms for network intrusion detection." AI in Cybersecurity (2019): 151-179. https://doi.org/10.1007/978-3-319-98842-9_6 [Accessed]

[33] Vinayakumar, Ravi, et al. "Deep learning approach for intelligent intrusion detection system." IEEE Access 7 (2019): 41525-41550. Doi: 10.1109/ACCESS.2019.2895334.[Accessed 25.04.2021].

[34] Weaver, Randy, Dawn Weaver, and Dean Farwood. Guide to network defense and countermeasures. Cengage Learning, 2013.

[35] Wang, Jie, and Zachary A. Kissel. Introduction to network security: theory and practice. John Wiley & Sons, 2015.

[36] Bioinformatics Web Development, "Internet and Networks", cellbiol.com [Online] Available: http://www.cellbiol.com/bioinformatics_web_development/ chapter-1- internet-networks-andtcp-ip/the-tcpip-family-of-internet-protocols/ [Accessed:17 July. 2021].

[37] Dua, Sumeet, and Xian Du. Data mining and machine learning in cybersecurity. CRC press, 2016., Introduction, Pg.1-114.

[38] E. Hildt, K. Lieb, and A. G. Franke, "Life context of pharmacological academic performance enhancement among university students–a qualitative approach," BMC medical ethics, vol. 1, no. 15, pp. 1-10., 2014. https://doi.org/10.1186/1472-6939-15-23

[39] Alghamdi, Mohammed I. "Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security." International Journal of Interactive Mobile Technologies 14.16 (2020). https://doi.org/10.3991/ijim.v14i16.16953. [Accessed 25.04.2021].

[40] J. B. Fraley and J. Cannady, "The promise of machine learning in cybersecurity," in South- eastCon 2017, 2017. https://doi.org/10.1109/secon.2017.7925283