Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 01 Issue: 02 | June-July 2024 | www.pumrj.com

Artificial Intelligence, Machine Learning, and Deep Learning for Cybersecurity Solutions: A Review of Emerging Technologies and Applications

Mallikarjuna Paramesha[1], Nitin Liladhar Rane[2], Jayesh Rane[3]

[1]Construction Management, California State University, Fresno, USA.
[2,3]University of Mumbai, Mumbai, India.

Abstract -The increasing intricacy and advancement of online dangers have required the creation of more advanced cybersecurity methods, with artificial intelligence (AI) becoming a crucial asset in this area. This document offers an in-depth overview of the most recent developments and upcoming technologies in AI-powered cybersecurity solutions, including machine learning (ML), deep learning (DL), natural language processing (NLP), and reinforcement learning (RL). Various aspects of cybersecurity utilize these AI technologies, including threat detection, response, network security, and data protection. The research carefully examines new studies to pinpoint main developments and uses, emphasizing the growing dependence on AI to tackle various cybersecurity issues. An examination of keyword co-occurrence uncovers the primary topics and connections in AI-driven cybersecurity studies, while a cluster analysis organizes these topics into separate subcategories, offering a systematic look at the research field. The results highlight the important contribution of AI in improving cybersecurity measures and provide useful guidance for future research. The integration of AI technologies is predicted to enhance security measures and drive innovation in diverse domains as cyber threats keep evolving.

Keywords: Cybersecurity, Artificial Intelligence, Network Security, Machine Learning, Deep Learning, Internet of Things, Learning Systems.

1.INTRODUCTION

The domain of cybersecurity has undergone a major change in the last few years due to the incorporation of artificial intelligence (AI) technologies. The increasing intricacy and advancement of online dangers have required the creation of more advanced security measures, with AI becoming a key tool in improving cybersecurity solutions [1]. Traditional security measures are often not enough to provide sufficient protection as cyber-attacks increase in frequency and complexity. AI shows potential in providing solutions to these challenges by analyzing large amounts of data and recognizing patterns. This article examines the most recent developments and up-and-coming technologies in AI-based cybersecurity solutions, with a focus on reviewing the literature, analyzing keyword co-occurrence, and clustering. The quick progress of AI technologies like machine learning, deep learning, natural language processing, and reinforcement learning has allowed for the creation of better cybersecurity solutions[2-3]. Various cybersecurity technologies are used in different areas such as threat detection, response, network security, and data protection. For example, machine learning algorithms can examine network data and identify irregularities that could signal possible cybersecurity issues. DL models, because they can learn from large datasets, are especially good at detecting complicated attack patterns and vulnerabilities that are new and have not been previously identified. NLP methods help in examining and understanding text data, assisting in threat intelligence and the detection of phishing attacks. Reinforcement Learning (RL), a branch of Machine

Learning (ML), is utilized in changing environments to improve security tactics and bolster decision-making procedures [4].

Recent research studies emphasize the incorporation of artificial intelligence in particular cybersecurity uses. AI-powered threat intelligence platforms, for instance, have the capability to review and interpret huge amounts of information from various origins, delivering instant insights on new dangers. AI is also being used more and more in endpoint security to identify and address malware and malicious behaviour on single devices technologies are utilized in network security to oversee and protect network infrastructures, identify intrusions, and handle access controls [5-8]. The rise of the Internet of Things (IoT) has broadened the range of AI applications in cybersecurity, as AI is now utilized to protect interconnected devices and smart environments [9-10].

The contributions of this research work are threefold:

- This study provides an in-depth review of the latest trends and advancements in AI-driven cybersecurity solutions, identifying key technologies and applications.
- By analyzing the frequency and relationships between key terms, this study offers insights into the main themes and areas of focus in the field.
- The study categorizes keywords into thematic groups, providing a structured overview of the research landscape and highlighting key areas of interest and potential avenues for future research.

2. METHODOLOGY

This research utilizes a qualitative approach, concentrating on an extensive review of the literature to investigate how artificial intelligence (AI) can improve cybersecurity solutions. The review methodically gathers, examines, and combines academic articles, industry reports, and case studies on AI-based cybersecurity technologies and applications. Keywords like "artificial intelligence", "machine learning", and "deep learning" were used in the search across databases such as Google Scholar, IEEE Xplore, and SSRN for topics like "cybersecurity", "network security", and "internet of things" regarding "threat intelligence", "cloud security", "identity and access management", and "incident response." Only scholarly journal articles, conference papers, and reliable industry reports from the past decade were reviewed to guarantee the findings' relevance and timeliness. The literature was grouped by main themes: AI and machine learning in cybersecurity, deep learning methods, natural language processing (NLP) for cybersecurity, reinforcement learning, AI for threat intelligence, AI in network security, AI for endpoint security, AI in cloud security, AI in identity and access management (IAM), and AI for incident response and management. This classification by theme made it easier to analyze the current research scene in an organized way. A study analyzing keyword co-occurrence was undertaken to discover the frequency and connections among important terms, displayed using a network graph. Highlighted were key terms such as "AI," "cybersecurity," "ML," "DL," and "IoT" due to their importance and frequency. This examination uncovered the primary topics and subjects of interest in AI-powered cybersecurity studies.

3. RESULTS AND DISCUSSION

Co-occurrence and cluster analysis of the keywords

Fig. 1 illustrates the connections and thematic groupings among various keywords, emphasizing their interrelations and central themes in AI-driven cybersecurity. Co-occurrence analysis reveals how frequently pairs of keywords appear together in the same context, represented by the nodes (keywords) and edges (co-occurrence) in the graph. Prominent keywords like "artificial intelligence," "cybersecurity," "internet of things," and "deep learning" are centrally positioned, indicating their significant role and frequent mention in relevant literature. The size of the nodes reflects the prominence of these keywords, with larger nodes indicating more frequently occurring terms. Cluster analysis organizes these keywords into thematic groups, shown in different colors, each representing a specific subfield or theme. For example, the blue cluster includes terms related to AI and machine learning, such as "learning algorithms" and "support vector machines," highlighting the technological foundation of AI in cybersecurity. The red cluster, containing keywords like "network security," "malware," and "intrusion detection," focuses on cybersecurity challenges and threats addressed by AI technologies. The green cluster, featuring "Internet of things," "smart city," and "cloud computing," underscores the intersection of AI, IoT, and cybersecurity, emphasizing the importance of securing interconnected environments. The purple cluster with keywords like "data security" and "privacy" highlights the critical need for data protection in AI applications. Finally, the yellow cluster includes emerging technologies and applications, such as "blockchain" and "federated learning," pointing to innovative methods for enhancing cybersecurity. This co-occurrence and cluster analysis offers a comprehensive overview of the research landscape, identifying key themes, gaps, and future research directions in leveraging AI for robust cybersecurity solutions.

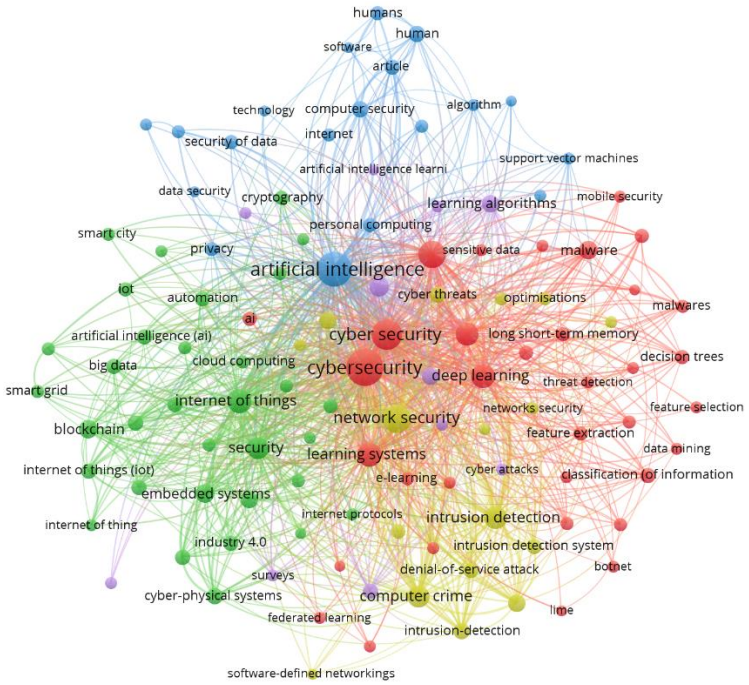

Fig -1: Co-occurrence analysis of the keywords in the literature

4. ARTIFICIAL INTELLIGENCE TECHNIQUES USED AS SOLUTIONS FOR CYBERSECURITY THREATS

AI has become essential in cybersecurity, providing advanced methods to combat complex cyber threats. Machine learning (ML), deep learning (DL), natural language processing (NLP), and reinforcement learning (RL) are some of the most influential AI techniques. Continuous improvements are being made to various technologies in order to better tackle cybersecurity challenges, offering strong protection against threats

through detection, response, and prevention. Machine learning, a branch of AI, has displayed great potential in recognizing and controlling cyber threats[11]. ML algorithms have the ability to examine large data sets in order to identify anomalies and patterns that may suggest malicious behavior. Supervised learning models are taught using past attack data to detect familiar threats, whereas unsupervised learning models can pinpoint new anomalies, offering preemptive defense measures. Methods like clustering and classification are frequently employed in machine learning to improve network security, identify intrusions, and oversee network traffic for potentially suspicious activity. Deep learning, a more sophisticated version of machine learning, utilizes neural networks containing numerous layers to handle and examine vast amounts of data. Fig 1. Shows the artificial intelligence techniques used as solutions for cybersecurity threats.

DL models excel at detecting intricate attack patterns and zero-day vulnerabilities, which are novel and previously undiscovered threats[12-13]. CNNs and RNNs are commonly used in cybersecurity for functions like identifying malware, detecting phishing attacks, and authenticating users. DL's capacity to acquire knowledge and adjust based on extensive unstructured data is a valuable asset in the fight against advanced cyber threats. NLP, an AI technique, is essential in cybersecurity. NLP involves the interaction between computers and human language, enabling systems to understand, interpret, and generate human language. NLP is utilized in cybersecurity to examine text data, like emails and social media content, for detecting phishing tries, social engineering assaults, and other forms of harmful communication. NLP models can detect questionable content and notify security teams about potential dangers by examining language semantics and context[14]. Table 1 shows the artificial intelligence techniques used as solutions for cybersecurity threats.

Table -1: Artificial intelligence techniques used as solutions for cybersecurity threats

Sr. No	AI Technique	Description	Applications in Cybersecurity	Advantages	Challenges
1	Machine Learning (ML)	A subset of artificial intelligence wherein algorithms are devised to infer patterns from data, thereby facilitating predictions or decision-making processes without explicit programming.	Employed in the detection of malware, the filtration of spam, the identification of anomalies, the implementation of intrusion detection systems (IDS), and the provision of predictive threat intelligence.	Exhibits high accuracy, adaptability to emerging threats, and the automation of repetitive security tasks.	Necessitates extensive datasets, susceptible to false positives and negatives, and vulnerable to adversarial attacks.
2	Deep Learning (DL)	An advanced segment of machine learning, characterized by neural networks with multiple layers, capable of analyzing intricate data patterns.	Utilized for the recognition of images in the context of malicious activity, natural language processing (NLP) for phishing detection, and sophisticated anomaly detection.	Proficient in handling extensive and complex datasets, ensuring high precision in pattern recognition, and effective in identifying zero-day exploits.	Computationally demanding, opaque in nature making explainability challenging, and reliant on large datasets for training.
3	Natural Language Processing (NLP)	A branch of AI focused on the comprehension and interpretation of human language by machines.	Applied in the detection of phishing emails, the analysis and classification of textual data in security logs, and the extraction of threat intelligence from unstructured data sources.	Effective in processing vast volumes of text, enhances threat detection capabilities, and improves incident response efficiency.	Ambiguities in natural language, necessitates continuous updates, and potential for misinterpretation of context.

4	Reinforcement Learning (RL)	A paradigm of machine learning wherein an agent learns to make decisions by interacting with its environment to achieve a specific goal.	Facilitates adaptive security measures, automated response systems, dynamic threat mitigation, and self-learning intrusion detection systems (IDS).	Learns optimal strategies, adapts to evolving environments, and minimizes human intervention.	Requires considerable training duration, may not generalize effectively to novel scenarios, and exhibits high complexity.
5	Anomaly Detection	A technique focused on identifying deviations from established norms to detect potential security threats.	Deployed in network traffic analysis, user behavior analytics, insider threat detection, and the identification of unusual access patterns.	Effective in detecting unknown threats, reduces false positives, and enhances the overall security posture.	May generate false alarms if normal behavior is not well-defined, and challenging to implement in dynamic environments.
6	Predictive Analytics	The utilization of historical data to forecast future events or behaviors, thereby enabling proactive threat management.	Employed in forecasting potential attacks, proactive threat hunting, identifying vulnerable systems, and conducting risk assessments.	Facilitates proactive threat management, improves preparedness, and enhances decision-making processes.	Dependent on the quality and relevance of historical data, and may not account for entirely novel types of threats.
7	Generative Adversarial Networks (GANs)	Involves the use of two neural networks in a competitive framework to generate realistic data, thereby enhancing training and improving security models.	Generates realistic attack scenarios for training, enhances threat detection models, and simulates potential attack vectors.	Augments the robustness of security models, improves training datasets, and aids in identifying system weaknesses.	Potentially exploitable for generating sophisticated attacks, computationally expensive, and complex to implement.
8	Support Vector Machines (SVM)	A supervised learning model used for classification and regression tasks, known for its ability to handle high-dimensional data.	Utilized in malware classification, intrusion detection, and distinguishing between legitimate and malicious activities.	Effective for small to medium-sized datasets, exhibits high accuracy in classification tasks, and robust against overfitting.	Less effective with large datasets, necessitates careful feature selection, and can be computationally intensive.
9	Decision Trees	A tree-structured algorithm used for decision-making and classification tasks, which splits data into branches to arrive at a decision.	Applied in identifying attack patterns, rule-based intrusion detection, and risk assessment.	Easy to interpret, handles both numerical and categorical data, and facilitates fast and efficient decision-making.	Prone to overfitting, may require pruning, and can become complex with extensive datasets.
10	Random Forest	An ensemble learning method that constructs multiple decision trees to enhance predictive accuracy and control overfitting.	Enhances malware detection, improves anomaly detection, and integrates multiple security metrics for comprehensive threat analysis.	Reduces overfitting, improves accuracy, and handles large datasets effectively.	Computationally intensive, less interpretable than individual decision trees, and necessitates careful parameter tuning.

Reinforcement learning, which is a subset of machine learning, centers on teaching agents how to choose actions by incentivizing good behaviors and discouraging bad ones. In cybersecurity, reinforcement learning is used in dynamic and intricate settings where security tactics need constant enhancement. For example, RL can be utilized to create adaptive intrusion detection systems that change by evolving threat environments. RL-based systems can optimize the distribution of cybersecurity resources, making sure that urgent and important threats are dealt with effectively and quickly. AI is being incorporated into threat intelligence platforms, improving their capacity to handle and analyze vast amounts of data from different origins[15]. These networks utilize artificial intelligence to offer immediate observations on upcoming dangers, aiding businesses in predicting and reacting to possible assaults. Moreover, AI methods are employed in endpoint security to identify and address malware and other malicious behaviors on individual devices. AI-powered endpoint security solutions can examine patterns of behavior and detect any abnormalities that could suggest a system has been compromised. AI is used in cloud security to oversee cloud environments, identify weaknesses, and handle access controls. AI technologies assist in protecting cloud infrastructure by offering automated capabilities for detecting and responding to threats, thus safeguarding cloud services against cyber threats. Moreover, AI has a crucial function in identity and access management (IAM) by aiding in the management of identities and regulating resource access. AI-powered identity and access management (IAM) tools can review user actions and identify irregularities, making sure that only approved users can reach confidential data[16-17].

The utilization of AI in incident response and management is equally remarkable. AI technologies can automatically identify and address cyber incidents, leading to faster response times and decreased damage from attacks. By using AI in incident response, organizations can improve their capacity to handle security breaches and bounce back from cyber incidents with greater efficiency. AI methods like machine learning, deep learning, natural language processing, and reinforcement learning are transforming the cybersecurity sector. These technologies offer enhanced features for identifying, reacting to, and stopping threats, enabling organizations to stay ahead of progressively more complex cyber-attacks. As artificial intelligence advances, its importance in cybersecurity is anticipated to grow, leading to new advancements and improving the efficiency of security measures in different fields[18].

Fig -1: Artificial intelligence techniques used as solutions for cybersecurity threats

5. MACHINE LEARNING FOR CYBERSECURITY SOLUTIONS

Machine learning (ML) is now seen as a fundamental aspect of modern cybersecurity approaches, offering effective solutions for identifying, stopping, and addressing cyber risks. ML algorithms are well-suited for cybersecurity due to their capability to analyze large datasets and detect patterns in the dynamic and complex nature of the field. This part delves into the newest and most influential uses of machine learning in improving cybersecurity protocols[19]. Anomaly detection is a key use of ML in the field of cybersecurity. Anomaly detection consists of detecting abnormalities in network traffic, user behaviors, or system operations. Supervised learning methods, depending on labeled datasets, are commonly employed to teach models to identify familiar dangers. One instance is when classification algorithms use past data to classify network traffic as either safe or harmful. Unsupervised learning methods like clustering and detecting outliers are just as beneficial because they don't need labeled data[20]. These models can detect uncommon patterns and alert to possible security incidents that have never been seen before. Machine learning is also crucial in intrusion detection systems (IDS) and intrusion prevention systems (IPS). These systems observe network traffic and examine it for indications of intrusion or malicious behavior. ML-based intrusion detection and prevention systems utilize a range of algorithms such as decision trees, support vector machines (SVM), and neural networks for real-time threat detection. Through constant exposure to updated information, these systems can adjust to changing dangers and enhance their precision as time goes on[21].

ML has demonstrated great effectiveness in the critical field of phishing detection. Phishing attacks, a common cybersecurity threat, trick users into disclosing sensitive information through deceptive emails or websites. ML algorithms can examine email content, URLs, and website features in order to identify phishing attacks. Methods like natural language processing (NLP) are used to analyze the text characteristics of emails, while machine learning models evaluate the layout and metadata of websites to detect deceptive ones. Being able to identify phishing scams promptly and effectively stops data breaches and safeguards user data[22].

ML plays an important role in detecting malware as well. Conventional methods of detecting malware through signatures face challenges in keeping up with the rapid growth of new malware variations. ML models can examine the actions of files and applications to detect malicious behavior. The behavioral analysis includes observing program behaviors like file access sequences, network links, and system changes. Through studying these actions, machine learning models can identify malicious software, including new types that have not been recognized before, by analyzing their behaviors instead of just depending on signatures. ML contributes significantly to network security by improving monitoring and threat detection capabilities. ML algorithms can examine patterns of network traffic to identify abnormalities that could signal a cyber-attack. For instance, ML models can use clustering techniques to categorize similar network traffic and detect outliers that might indicate a potential attack. Moreover, machine learning can also forecast potential weaknesses and ways for attackers to exploit them by examining past data and recognizing patterns[23].

Within the area of endpoint security, machine learning offers strong solutions for safeguarding individual devices against cyber threats. EDR systems utilize machine learning to observe device actions and identify potentially harmful activities. These systems can recognize and minimize dangers like ransomware, which frequently displays distinct behavior patterns on compromised devices. ML-based EDR systems can adapt to new attack techniques and offer proactive protection by constantly learning from fresh data. Identity and access management (IAM) is a field in which ML improves security measures. ML models can examine user actions and identify irregularities that could suggest compromised accounts or unauthorized access

attempts. By understanding the habits of users, like the times they log in and where they access information, ML can identify any unusual behavior that needs to be looked into. This proactive method aids in preventing unauthorized entry and safeguarding sensitive data. ML also plays a crucial role in the creation of cutting-edge threat intelligence platforms. These platforms collect and process data from different sources like threat feeds, logs, and social media to offer instant insights on new threats. ML algorithms can recognize patterns and connections in this data, allowing security teams to better predict and address potential attacks. machine learning is now a crucial component of cybersecurity solutions, providing enhanced functions for identifying, stopping, and addressing threats. Its use in anomaly detection, intrusion detection, phishing detection, malware detection, network security, endpoint security, and identity and access management has greatly improved organizations' ability to safeguard their digital assets. The evolution of cyber threats is leading to an increasing role of machine learning in cybersecurity, which is anticipated to enhance innovation and boost the effectiveness of security measures in different fields[24-25].

6. DEEP LEARNING FOR CYBERSECURITY SOLUTIONS

Deep learning (DL), a branch of machine learning (ML), has transformed the cybersecurity industry by efficiently analyzing large datasets and detecting complex patterns that traditional techniques frequently overlook. By utilizing deep learning models with numerous layers of neural networks, complex data representations can be learned effectively, making them highly efficient in identifying and minimizing advanced cyber threats. This part delves into the most recent uses and developments in deep learning to improve cybersecurity solutions. The detection of malware is one of the most important uses of deep learning in cybersecurity. Conventional methods of using signatures have difficulty keeping up with the fast growth of new forms of malware[26]. On the other hand, deep learning models like CNNs and RNNs can examine the traits and actions of data to identify malicious software. CNNs are very good at analyzing binary file structures and finding malicious code due to their skill in recognizing spatial hierarchies in data. RNNs are proficient at handling sequential data and can examine sequences of system calls and patterns in network traffic to detect abnormal behaviors that may signal the presence of malware. Deep learning has also had a significant impact in intrusion detection systems (IDS) and intrusion prevention systems (IPS). DL models improve these systems by increasing accuracy in detecting potential intrusions and reducing false positives[27]. Autoencoders, which are a type of unsupervised deep learning model, are commonly utilized for detecting anomalies in network traffic. These models can identify anomalies that suggest a possible intrusion by learning a condensed version of regular network activity. Additionally, the application of deep belief networks (DBNs) and deep neural networks (DNNs) is utilized for the classification of network traffic as either normal or malicious, allowing for prompt threat identification and reaction.

Phishing detection is also significantly influenced by deep learning. Phishing attacks, a significant worry in cybersecurity, trick users into revealing sensitive information. DL models can examine the content of emails, URLs, and characteristics of web pages to identify phishing attempts. NLP methods, enhanced by DL, are used to analyze the text in emails, spotting questionable language patterns and signs of deception. Furthermore, DL models are capable of examining the structural and visual aspects of websites to differentiate between authentic and deceptive sites, offering a strong defense against phishing attempts[28,29]. Deep learning is employed in user and entity behavior analytics (UEBA) to identify abnormal actions that could signal insider threats or compromised accounts. LSTM networks, a kind of RNN, excel at modeling user behavior across periods. These networks can understand the usual behavior patterns of users and identify irregularities indicating possible malicious activities. LSTM networks aid in

detecting potential security breaches and unauthorized access attempts by examining login times, access patterns, and transaction behaviors continually. Deep learning has improved threat intelligence platforms through its ability to analyze vast amounts of unstructured data from various sources. DL models can analyze information from sources like threat feeds, social media, and dark web forums to detect new threats and offer useful insights. These models can identify intricate patterns and relationships in the data, providing advance alerts and facilitating preemptive defense actions[30].

Deep learning models are used in endpoint security to supervise and safeguard individual devices. DL-driven EDR systems are able to examine how applications and processes behave on endpoints, detecting indicators of compromise like abnormal file access patterns or unauthorized network connections. These systems use deep learning to offer instant identification and prevention of risks, guaranteeing strong defense for endpoints. The incorporation of deep learning into identity and access management (IAM) has led to notable progress. DL models can improve authentication mechanisms and detect anomalies by analyzing user behavior and contextual information. DL-based systems can reduce unauthorized access risks by analyzing historical login data to detect suspicious login attempts and adjust security policies accordingly. Deep learning is utilized for monitoring cloud environments and identifying vulnerabilities in cloud security. DL models are capable of examining cloud infrastructure setups, user behaviors, and network communication to detect possible security vulnerabilities. These models offer automated detection and response features to safeguard cloud services from evolving cyber threats[31].

Deep learning is now a fundamental component of contemporary cybersecurity solutions, providing enhanced functionalities for identifying, stopping, and addressing threats. Its uses in detecting malware, intrusions, phishing attacks, analyzing user behavior, providing threat intelligence, securing endpoints, and managing identity and access have greatly improved organizations' ability to protect their digital resources. With the increasing complexity of cyber threats, deep learning is anticipated to play a larger role in cybersecurity, leading to advancements and enhancing the effectiveness of security measures in different areas[32].

7. NATURAL LANGUAGE PROCESSING (NLP) IN CYBERSECURITY SOLUTIONS

Natural Language Processing (NLP) is a sector of artificial intelligence (AI) which concentrates on the communication between computers and human language, and has now become a crucial component of cybersecurity tactics. NLP offers effective tools for identifying and reducing cyber threats that take advantage of textual and communicative data by allowing systems to comprehend, interpret, and produce human language. This part delves into the most recent uses and shifts in NLP to improve cybersecurity solutions. Phishing detection is a key use of NLP in cybersecurity. Deceptive emails intended to trick recipients into revealing sensitive information, known as phishing attacks, are a significant security issue. NLP methods examine the text in emails to detect unusual language patterns, misleading signals, and irregularities. For example, models have the capability to identify small differences in email format, grammar, and word choice that signal potential phishing attacks. By utilizing NLP, security systems have the capability to identify suspicious emails before they are delivered to the recipients, thus avoiding data leaks and safeguarding user data[33-34]. Fig 2. Shows the Natural Language Processing (NLP) in cybersecurity solutions.

Another important use of NLP in the field of cybersecurity is in threat intelligence. NLP methods are utilized for handling and examining extensive amounts of unorganized data from various origins like social media, forums, and dark websites. NLP models can recognize new dangers, monitor threat actors, and offer useful

insights by extracting pertinent details from text data. One instance where NLP is utilized is to keep track of hacker forums for conversations regarding fresh vulnerabilities or upcoming attacks. Security teams can obtain early warnings and proactively address potential threats by comprehending the context and sentiment of conversations. NLP plays a crucial role in examining and reducing social engineering attacks as well. These attacks exploit human interactions in order to obtain unauthorized access to information or systems. NLP models have the ability to examine conversational data like chat logs and voice recordings in order to identify indications of social engineering[35]. Methods such as sentiment analysis and emotion detection are useful in detecting efforts to deceive or manipulate users. NLP can help security teams identify patterns of social engineering and stop potential exploitation by alerting them to suspicious interactions.

NLP can be utilized in malware detection to analyze threats from code and scripts. NLP techniques can be used to detect linguistic patterns and commands within malicious scripts. By analyzing the structure and meaning of these codes, NLP models can distinguish between harmless and harmful scripts. This feature is especially handy for identifying file-less malware and scripts that are hidden in documents or web pages. UEBA's enhancement is also significantly influenced by NLP's involvement[36]. NLP models can create behavior profiles for users and entities by studying written interactions like emails and chat messages. Any departures from these profiles may be identified as possible security breaches. If an employee usually uses formal language in emails but suddenly begins using informal or urgent language, it could mean their account has been hacked. NLP-powered UEBA assists in detecting anomalies and stopping insider threats and account takeovers.

In the realm of automated incident response, NLP can aid in quickly analyzing security alerts and logs. SIEM systems produce large volumes of text data that require analysis to detect and address threats. NLP methods, like text classification and clustering, are useful in arranging alerts by importance and linking associated incidents. This allows for a quicker and more efficient response to incidents, decreasing the window of opportunity for attackers to exploit weaknesses. Moreover, NLP improves authentication mechanisms to enhance identity and access management (IAM). One example is how NLP is utilized in voice recognition systems to evaluate users and verify their identity through speech patterns[37-39]. In the same way, natural language processing can be employed to examine user inquiries and directives in natural language interfaces, guaranteeing that only approved individuals can access confidential information and systems.

NLP is now a crucial aspect of contemporary cybersecurity solutions, providing advanced features for detecting, avoiding, and responding to threats. Its uses in detecting phishing, identifying threats, reducing social engineering, finding malware, analyzing user behavior, responding to incidents automatically, and managing identity and access greatly improve organizations' ability to safeguard their online assets. The expanding role of NLP in cybersecurity is expected to drive innovation and enhance security measures in different areas as cyber threats evolve[40].

Fig -2: Natural Language Processing (NLP) in cybersecurity solutions

8. REINFORCEMENT LEARNING IN CYBERSECURITY SOLUTIONS

Receiving rewards or penalties for their actions, agents in reinforcement learning (RL) - a subset of machine learning - are increasingly popular in the cybersecurity field. Continuously adjusting to fresh data and changing dangers, RL offers flexible and strong answers for different cybersecurity issues. This part looks into the newest uses and patterns in reinforcement learning to improve cybersecurity solutions. Reinforcement learning is commonly used in cybersecurity for creating adaptive systems like intrusion detection systems (IDS) and intrusion prevention systems (IPS). Conventional IDS/IPS systems typically depend on fixed rules and signatures, which can be bypassed by advanced attackers. RL-driven systems have the ability to adapt their detection strategies in response to live feedback[41]. RL models can enhance their ability to detect by recognizing new attack patterns through environmental learning. The flexibility of RL makes it a powerful weapon in identifying and stopping various cyber threats.

RL is employed in network security for optimizing resource allocation and configuration management in networks. For instance, RL algorithms can be used to adjust firewalls and intrusion detection rules in real-time, guaranteeing that the network is safeguarded from the most pressing dangers. Through ongoing analysis of network traffic and attack patterns, RL models have the capability to anticipate possible weaknesses and proactively enhance defenses[42]. This proactive method helps to keep the network environment safe and minimize any negative effects on performance. Reinforcement learning is also important in automated threat hunting. Threat hunting is the proactive search for patterns of malicious behavior in a network, as opposed to simply reacting to alerts. RL models have the capability to be trained to maneuver through intricate network surroundings and detect signs of compromise. RL agents learn to differentiate between regular and suspicious behavior by receiving rewards for accurately identifying threats and punishments for false positives. This ability improves the efficiency of hunting for threats and shortens the time needed to identify and address cyber threats[43].

Another important use of RL in cybersecurity involves detecting and reducing malware. RL models are capable of being trained to identify harmful actions and respond effectively to eliminate dangers. An example is when RL agents observe system operations and network links, spotting and stopping harmful

actions immediately. Moreover, RL can also be applied to create self-repairing systems that can recover from attacks without human intervention. These systems can achieve regular functioning with minimal human involvement by mastering the best recovery measures. RL offers advanced solutions for securing individual devices from cyber threats in the realm of endpoint security. EDR systems use RL to constantly watch device behaviors and identify abnormalities. RL agents possess the ability to understand the typical behavior patterns exhibited by applications and users, alerting when any abnormal behaviors are detected that could suggest a security breach. This method makes sure that endpoints are shielded from emerging threats and lowers the chances of attacks being successful[44-45].

Reinforcement learning is used in managing access controls and verifying identities. RL models have the ability to evaluate user actions and adjust security verification methods according to the level of potential danger. For instance, when an RL agent notices abnormal login patterns or access requests, it has the ability to implement more stringent authentication processes or temporarily limit access. This active method of managing identity and access (IAM) aids in preventing unauthorized entry and improving overall security. In the field of incident response, RL has the ability to automate decision-making in security incidents. RL agents are able to assess the seriousness of a situation and decide on the best course of action to take. RL models can improve response strategies and speed up recovery by studying past incidents and results. This automation alleviates the workload of security teams and enhances the effectiveness of incident response operations[46].

Furthermore, the use of RL is on the rise in improving threat intelligence platforms. These platforms collect and evaluate information from different origins in order to offer an understanding of upcoming dangers. RL models can be taught to recognize patterns and connections in the data, providing anticipatory guidance to organizations in preventing and managing possible attacks. RL-enhanced threat intelligence platforms offer current and actionable information for proactive defense by constantly learning from new data. reinforcement learning is revolutionizing cybersecurity solutions, offering active and flexible tools for identifying, stopping, and reacting to threats. Its usage in intrusion detection, network security, threat hunting, malware detection, endpoint security, access control management, incident response, and threat intelligence greatly improves organizations' ability to safeguard their digital assets. The evolution of cyber threats will likely lead to an increased use of reinforcement learning in cybersecurity, which will drive innovation and enhance the effectiveness of security measures in different fields[47-48].

9. ARTIFICIAL INTELLIGENCE FOR THREAT INTELLIGENCE SOLUTIONS IN CYBERSECURITY

In the field of threat intelligence, artificial intelligence (AI) has grown into a vital resource, providing advanced technology to identify, assess, and address cyber threats instantly. By utilizing artificial intelligence, companies can improve their ability to detect and defend against threats, leading to better cybersecurity protection. This part delves into the most recent uses and developments in AI-based threat intelligence solutions[49].

Automated analysis of large volumes of data is one of the major uses of AI in threat intelligence. Conventional threat intelligence techniques typically require manual procedures that are time-consuming and susceptible to human error. AI models, specifically machine learning (ML) and deep learning (DL) models, are able to handle and examine vast amounts of data from various origins such as network logs, social media, and dark web forums. These models have the ability to detect patterns and relationships that could suggest potential dangers on the horizon. AI has the capability to identify abnormal network traffic trends or unusual actions indicating a possible cyber threat, enabling security teams to proactively intervene[50]. Natural language processing (NLP), which is a branch of artificial intelligence (AI), is

especially adept at threat intelligence. NLP methods are able to examine text data from a range of origins like threat reports, security blogs, and hacker forums to retrieve pertinent information and understandings. By comprehending the context and meanings of the language employed in these texts, NLP models can detect novel vulnerabilities, exploit techniques, and intended attacks. This feature enables organizations to outsmart malicious actors and enhance their protection against possible vulnerabilities[51].

AI improves the precision and pace of identifying threats by automating the matching and examination of threat information. SIEM systems are now integrating AI to enhance their efficiency as they gather and analyze security data from various parts of the organization. AI algorithms have the capability to connect occurrences from various origins, detect irregularities, and rank risks according to their seriousness and possible consequences. This automated correlation assists in decreasing the number of incorrect alerts and guarantees that important threats are dealt with quickly. AI is essential in predicting possible cyber threats in the field of predictive threat intelligence. Through the examination of past data and the detection of patterns, AI models can forecast upcoming attack strategies and malicious actor actions. Anticipatory analytics empower organizations to predict potential dangers and put safeguards in place before an attack takes place. One instance is when AI can forecast the chance of specific types of attacks, like phishing or ransomware, by analyzing past trends and current threat conditions. This ability to anticipate enables security teams to allocate resources more efficiently and improve their readiness[52-53].

AI-powered threat intelligence platforms are also critical in improving situational awareness. These platforms collect information from various sources and offer a cohesive perspective of the threat environment. AI algorithms examine this information to create useful insights, like recognizing compromised accounts, identifying data exfiltration actions, and revealing signs of compromise (IoCs). This thorough understanding of the situation allows organizations to react to threats more effectively and reduce the consequences of cyber incidents. Another important use of AI in threat intelligence involves recognizing and examining Advanced Persistent Threats (APTs). APTs are advanced and focused cyber-attacks designed to obtain long-term access to a network. AI models can identify the subtle and extended actions connected to APTs through constant observation of network traffic and user actions. Machine learning models, especially anomaly detection methods, are capable of recognizing abnormal behavior that could signal an APT attack. AI assists in reducing the impact of APTs and stopping major data breaches by identifying these patterns at an early stage[54].

AI also aids in the sharing of threat intelligence and partnerships between organizations. AI allows organizations to quickly share information on new threats and vulnerabilities by standardizing and automating the collection and distribution of threat intelligence. This cooperative method strengthens joint protection against cyber threats and enhances the overall security environment. AI-driven platforms can automatically consume threat intelligence feeds, study the information, and provide the necessary details to the relevant parties, guaranteeing quick and efficient reactions. Artificial intelligence is changing threat intelligence solutions by offering enhanced features for identifying, examining, and addressing threats. The use of automated data analysis, natural language processing, predictive threat intelligence, situational awareness, and APT detection greatly improves organizations' ability to safeguard their digital assets. The increasing complexity and frequency of cyber threats are expected to lead to a growing role of AI in threat intelligence, which will drive innovation and enhance cybersecurity resilience in various sectors[55-56].

10. ARTIFICIAL INTELLIGENCE SOLUTIONS IN NETWORK SECURITY

Artificial intelligence (AI) has transformed network security through the provision of sophisticated tools and methods for identifying, stopping, and addressing cyber threats. By utilizing AI, companies can improve

their network security defenses, guaranteeing strong protection against ever-evolving cyber threats. This part examines the most recent uses and developments in AI-powered network security solutions. Anomaly detection is a key use of AI in network security. Conventional security systems typically depend on established rules and signatures, which could be evaded by emerging threats. Artificial intelligence, specifically machine learning (ML) models, is highly skilled at detecting abnormalities that differ from typical network patterns. These models have been trained using huge volumes of network traffic data in order to identify patterns and identify anomalies that might indicate potential threats. For instance, unsupervised learning methods like clustering and outlier detection can find abnormal traffic patterns that might indicate a security breach or an outbreak of malware. AI systems can evolve to address emerging threats and offer immediate detection and response by consistently learning from network data[57].

Deep learning (DL) models, a subset of artificial intelligence (AI), have greatly enhanced the functions of intrusion detection systems (IDS) and intrusion prevention systems (IPS). These models, such as CNNs and RNNs, are able to examine extensive amounts of network data in order to detect intricate patterns of attacks. CNNs excel at identifying spatial hierarchies in data, which makes them ideal for detecting harmful content in network packets. RNNs are created for handling sequential data and can examine sequences of network events to identify intrusions occurring gradually. By utilizing deep learning, IDS/IPS can improve accuracy in threat detection and lower the number of false positives. AI also plays a key role in improving firewall and access control systems. Next-gen firewalls utilize artificial intelligence to assess network traffic and determine whether to permit or restrict it. These firewalls utilize machine learning algorithms to analyze packet data, evaluate risk levels, and apply security policies in real-time. AI-powered firewalls can detect and prevent advanced threats like zero-day attacks and APTs by utilizing historical data and real-time analysis, which traditional firewalls may overlook[58-59].

In the realm of threat hunting, artificial intelligence offers effective tools for actively searching for indications of malicious activities within a network. Threat hunting entails examining network traffic, system logs, and additional data sources in order to reveal concealed threats. AI-powered threat detection platforms utilize machine learning algorithms to uncover patterns and irregularities signaling possible security breaches. These platforms are able to connect information from various sources, offering a complete perspective of the network's security status. AI decreases the time and effort needed to identify and address threats by automating the threat-hunting process. AI is important in improving network security by automatically responding and fixing issues. SOAR platforms utilize artificial intelligence to automatically investigate and address security incidents. AI-powered SOAR systems can activate pre-defined playbooks to control and lessen the impact of a detected threat. For instance, an AI system could isolate a compromised device from the network, block malicious IP addresses, and start incident response procedures automatically. This system cut down on response times and lessens the effects of security incidents[60].

AI allows for constant and thorough monitoring of network activities in the field of network surveillance. ML algorithms are utilized by AI-based network monitoring tools to analyze network traffic in real-time, identifying anomalies and potential threats. These tools are able to detect slight signs of compromise, like abnormal login activities, data theft attempts, and moving laterally across the network. AI-powered monitoring solutions improve security team's response to threats by offering real-time alerts and actionable insights. AI is used for securing both IoT devices and networks. IoT devices frequently lack robust security measures, leaving them susceptible to cyber attacks. AI has the potential to improve IoT security through the surveillance of device actions and the identification of irregularities that could signal a security breach. For instance, machine learning algorithms have the capability to examine the communication behaviors of Internet of Things (IoT) devices in order to spot any abnormal behaviors like unauthorized data

transfers or unanticipated links. AI assists in safeguarding IoT networks to shield critical infrastructure and confidential data from cyber dangers[61].

Moreover, AI-powered technology is used in network forensics for the examination and analysis of previous security breaches. AI models can analyze extensive amounts of past network data to reconstruct the series of events that led to a security breach. This forensic examination assists in pinpointing the main reason behind incidents, grasping the tactics, techniques, and procedures (TTPs) employed by attackers, and enhancing upcoming defenses. AI improves organizations' capacity to understand and learn from past incidents, thus reinforcing their security defenses. use of artificial intelligence is revolutionizing network security through enhanced abilities in detecting, preventing, and responding to threats. Utilizing it can greatly enhance organizations' capability to safeguard their digital assets through various uses such as anomaly detection, intrusion detection, firewall enhancement, threat hunting, automated response, network monitoring, IoT security, and network forensics. With the continuous evolution of cyber threats, the use of AI in network security is anticipated to grow, leading to innovation and enhancing the strength of security measures in different areas[62-63].

11. ARTIFICIAL INTELLIGENCE FOR ENDPOINT SECURITY SOLUTIONS

The use of Artificial intelligence (AI) in endpoint security is growing, offering advanced features for identifying, stopping, and addressing cyber threats directed at specific devices on a network. By utilizing artificial intelligence, companies can improve their endpoint security, guaranteeing full coverage against advanced attacks. This part delves into the most recent uses and developments in AI-powered endpoint security solutions. AI in endpoint security has a key focus on detecting and preventing malware[64]. Conventional antivirus programs typically depend on recognizing specific signatures to detect threats, but these can be circumvented by advanced or shape-shifting malware. AI, especially machine learning (ML) models, is very good at detecting harmful actions by examining the attributes and actions of files and applications. AI systems can detect new malware by identifying abnormal patterns and behaviors through techniques like anomaly detection, classification, and clustering. One example is the use of ML algorithms to examine file attributes, system calls, and network connections in order to identify suspicious behavior, even when the malware does not have a recognized signature[65].

Deep learning models, which are a part of artificial intelligence (AI), improve the ability to detect malware by analyzing vast amounts of data to pinpoint intricate patterns. CNNs and RNNs excel in examining both the fixed and changing attributes of files. CNNs have the ability to analyze the composition of executable files in order to find hidden harmful code, while RNNs can observe patterns of system activities to pinpoint active cyber threats. Through the use of DL, endpoint security solutions can improve their ability to detect advanced malware and decrease the occurrence of incorrect detections. AI plays a key role in identifying and minimizing advanced persistent threats (APTs) on endpoints. APTs are extended, focused attacks with the goal of stealing data or causing disruptions. AI-powered EDR systems monitor endpoint activities constantly, utilizing machine learning algorithms to spot abnormalities that may suggest an advanced persistent threat (APT). These systems are able to identify subtle indications of breach, like irregular file access patterns, unanticipated network connections, and deviations from typical user behavior. AI-driven EDR solutions can rapidly detect and control APTs by monitoring these indicators in real-time, thus reducing their impact[66]. Fig 3. Shows the artificial intelligence for endpoint security solutions.

AI improves endpoint security by creating thorough profiles of typical user and device behaviors within the realm of behavioral analysis. Machine learning algorithms have the ability to understand common usage patterns like login times, application usage, and network access, and can identify unusual behavior that

could signal a security breach. For instance, if a device begins showing behavior that doesn't match its usual patterns, like accessing confidential documents it doesn't usually access, the AI system can produce a notification for more examination. This proactive method aids in detecting insider threats and compromised accounts. AI is essential in improving endpoint security by providing automated responses and solutions to threats. SOAR platforms utilize artificial intelligence to automate the response and investigation of threats that are discovered on endpoints. When a potential threat is detected by an AI-powered endpoint security system, it has the ability to isolate the affected device, stop harmful processes, and eliminate malicious files automatically. This automation lowers response times and guarantees that threats are eliminated before they can create substantial harm[67-68].

In the sphere of phishing detection, artificial intelligence offers strong solutions for safeguarding endpoints against email-based attacks. Phishing emails are frequently used as a method to distribute malware or obtain login information. AI models, especially ones utilizing natural language processing (NLP), have the capability to examine email content in order to identify phishing efforts. These models analyze different components of the email, such as the language utilized, the format of URLs, and the sender's credibility, in order to detect malicious intentions. AI improves endpoint security by blocking phishing emails, which helps prevent users from accidentally putting their devices at risk. AI-powered endpoint security solutions provide advanced features for the management and protection of mobile devices as well. Securing mobile endpoints is now more crucial due to the widespread adoption of bring-your-own-device (BYOD) policies. AI algorithms are capable of observing mobile device actions, like installing apps, connecting to networks, and accessing data, in order to identify any unusual patterns that could signal a security breach. AI guarantees that mobile endpoints stay protected even when not connected to the corporate network by offering instant threat identification and automatic response[69].

Furthermore, AI improves endpoint security by integrating threat intelligence. AI-powered systems are able to consume threat intelligence feeds from different origins, evaluate the information, and connect it with endpoint behaviors. This integration allows for the detection of emerging threats by analyzing worldwide threat patterns and indicators of compromise (IoCs). AI-powered endpoint security solutions can outsmart new threats and offer current protection by utilizing threat intelligence. artificial intelligence is changing endpoint security by offering enhanced abilities for detecting, preventing, and responding to threats. The use of this technology greatly improves organizations' ability to defend their endpoints through tasks like detecting malware, mitigating APTs, analyzing behavior, responding automatically, detecting phishing attempts, securing mobile devices, and gathering threat intelligence. With the ever-changing landscape of cyber threats, AI is projected to play a larger role in endpoint security, leading to increased innovation and enhanced security resilience in different sectors[70-71].

Fig -3: Artificial intelligence for endpoint security solutions.

12. ARTIFICIAL INTELLIGENCE SOLUTIONS IN CLOUD SECURITY

AI plays a growingly important role in cloud security, offering advanced tools to protect cloud environments from various cyber threats. By utilizing AI, companies can improve their cloud security protocols, guaranteeing strong defense for data, applications, and services stored in the cloud. This part examines the most recent uses and developments in cloud security solutions driven by AI[72]. One major use of AI in cloud security is identifying and stopping unusual behaviors. Monitoring and identifying threats manually becomes difficult in cloud environments due to the huge volume of data they generate. AI, especially ML algorithms, is very good at examining vast amounts of data to uncover abnormal patterns and behaviors. These algorithms have the ability to understand usual cloud workload patterns and identify changes that could signal possible security risks. For instance, clustering and anomaly detection in unsupervised learning can swiftly detect abnormal login attempts, unauthorized data access, and other potentially risky activities, allowing quick mitigation actions. Deep learning models, which are a part of artificial intelligence (AI), improve the ability to detect threats in cloud security. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are adept at analyzing intricate data structures and sequences, which makes them highly efficient at detecting sophisticated threats[73]. CNNs are capable of identifying abnormalities in network traffic and application behavior, while RNNs can examine time-series data to recognize patterns and forecast possible security breaches. Through the utilization of deep learning, cloud security solutions can enhance their ability to detect threats with greater precision and lower the occurrence of false alarms, thus ensuring more dependable security for cloud environments.

AI plays a crucial role in ensuring the security of cloud infrastructure by automating configuration management and monitoring compliance. Misconfigurations frequently lead to cloud security breaches, typically caused by human mistakes or lack of attention. AI-powered tools are able to constantly observe cloud setups to make sure they follow security guidelines and meet compliance standards. Machine learning algorithms are capable of detecting misconfigurations like overly permissive access controls or

unencrypted data storage and recommending ways to fix them. Furthermore, AI has the capability to automatically implement security policies, minimizing the chance of errors and guaranteeing the security and compliance of cloud environments[74-75]. Within the field of identity and access management (IAM), AI improves security through offering adaptive methods for authentication and authorization. Artificial intelligence (AI) models are able to examine user actions and surrounding context in order to identify irregularities and modify access restrictions as needed. For example, if an AI system identifies a strange login try from an unknown place or gadget, it can implement multi-factor authentication (MFA) or limit access temporarily. This proactive method of IAM aids in stopping unauthorized entry and safeguarding sensitive information stored in the cloud.

AI-powered solutions are also essential in threat intelligence for securing the cloud. AI can offer immediate insights into new risks and weaknesses by gathering and studying data from different sources. AI algorithms are able to link threat information with actions in the cloud in order to detect signs of compromise and possible avenues for attack. This proactive threat intelligence allows organizations to predict and address threats before they affect cloud environments. Moreover, AI can improve incident response by offering practical suggestions derived from examining past attack information. In the field of data security, AI provides sophisticated encryption and data loss prevention (DLP) options. Artificial intelligence models have the capability to examine data streams and recognize sensitive data that requires safeguarding. Machine learning algorithms have the ability to identify signs of data exfiltration attempts and can implement encryption or other protective measures automatically. AI-powered DLP solutions can also oversee data access and usage, guaranteeing that sensitive data is not disclosed or leaked. AI assists in safeguarding vital assets in cloud environments by automating data protection and thwarting unauthorized access to data[75].

Another important use of AI in cloud security involves automating the response and fixing of threats. SOAR platforms utilize artificial intelligence to automate the examination and resolution of security incidents in the cloud. AI-powered SOAR systems can run pre-established playbooks to thwart and address detected threats. For instance, an AI system could autonomously isolate a hacked virtual machine, revoke access credentials, and start forensic investigation. This automated system decreases the amount of time it takes to respond and guarantees that dangers are stopped before they can inflict substantial harm. AI is additionally employed to improve the security of cloud-based applications and services. Incorporating AI into DevSecOps practices ensures that security is a priority throughout the software development lifecycle. AI-powered tools have the ability to examine code for weaknesses, observe how applications behave, and identify security concerns in the process of development and deployment. By integrating AI into DevSecOps, companies can guarantee that their cloud-native apps are built with security in mind and can withstand changing threats[76-77]. Artificial intelligence is changing cloud security by offering advanced capabilities to detect, prevent, and respond to threats. Its uses in anomaly detection, automated configuration management, adaptive IAM, threat intelligence, data protection, automated threat response, and DevSecOps greatly improve organizations' capability to safeguard their cloud environments. The increasing complexity of cyber threats is projected to boost the utilization of AI in cloud security, leading to enhanced security measures and advancements in various fields[78].

13. ARTIFICIAL INTELLIGENCE IN IDENTITY AND ACCESS MANAGEMENT (IAM) SOLUTIONS

Artificial intelligence is changing Identity and Access Management by offering innovative tools and methods to protect and control user identities and access privileges in a company. By utilizing AI, companies can improve their IAM tactics, strengthening defenses against unauthorized entry and

enhancing overall security measures. This part investigates the most recent uses and developments in AI-powered IAM solutions[79]. AI plays a major role in adaptive authentication within IAM. Conventional methods of verification frequently depend on unchanging credentials like passwords, which are easily vulnerable to compromise. AI implements authentication mechanisms that are responsive to changing circumstances and assess multiple factors before allowing entry. Machine learning models use user behavior patterns, like login times, locations, and device types, to assess the risk of every access attempt. For instance, when a user tries to access their account from a new location or device, the AI system may require additional authentication measures like multi-factor authentication (MFA). This flexible method aids in the prevention of unauthorized entry and safeguards confidential data. AI also improves the verification of identities by including biometric authentication techniques. Biometric information, like fingerprints, facial recognition, and voice recognition, offers greater security than standard credentials. AI models accurately process and analyze biometric information to confirm user identities. An illustration of this is when facial recognition systems employ deep learning (DL) algorithms to scrutinize facial characteristics and compare them to saved profiles. It is challenging to trick this biometric verification, which makes it a trustworthy way to protect important systems and information[80-81]. Fig 4. Shows the artificial intelligence in Identity and Access Management (IAM) Solutions.

AI is essential for implementing changing access controls in access management. Conventional access control systems frequently rely on fixed roles and permissions that may become obsolete as organizational requirements evolve. AI-powered IAM solutions constantly examine user roles and access behaviors to modify permissions instantly. Machine learning algorithms are capable of detecting unusual access requests, like when an employee retrieves data beyond their usual job duties, and can promptly modify access controls to reduce possible threats. This active method guarantees users have the correct level of access according to their existing roles and responsibilities. AI plays a key role in identifying and stopping insider threats in IAM. Insider threats, involving employees or contractors abusing their access privileges, present high levels of risk for organizations. AI models have the ability to examine user actions and identify irregularities that could signal potentially harmful behavior. One scenario is when an employee starts accessing a large amount of confidential data out of the blue or tries to download restricted files, the AI system can mark this conduct for additional scrutiny. AI assists in detecting and preventing insider threats by observing user behavior in real-time to prevent potential damage[82-83].

Furthermore, AI improves IAM by automating the management of identity lifecycles, in addition to identifying insider threats. Overseeing user identities from start to finish, including adding and removing access, is a intricate process that necessitates careful focus. AI-powered identity and access management solutions automate various parts of managing identity lifecycles, including setting up and removing user accounts. Machine learning algorithms are able to examine patterns in user roles and access requirements in order to simplify the provision process, guaranteeing that new employees possess the required access right from the start. Likewise, AI can streamline the de-provisioning procedure for departing employees, minimizing the potential for unused accounts that may be abused. AI-powered IAM solutions also incorporate threat intelligence to improve security measures. By examining threat information from different origins, AI can detect developing dangers and modify IAM regulations as needed. For instance, when a specific kind of phishing attack is becoming more common, the AI system can enhance the strictness of authentication steps for users who may be targeted. This proactive method makes sure that IAM policies stay current and continue to be effective in the face of changing threats[84-85].

Moreover, AI enhances IAM efficiency by lessening the workload for IT and security teams. Conventional IAM systems frequently need human involvement to handle access requests, reset passwords, and investigate

security incidents. AI streamlines a lot of these tasks, enabling IT and security staff to dedicate their attention to more strategic activities. For example, chatbots powered by AI can manage basic access requests and password resets, offering instant help to users and allowing IT resources to be available for other tasks. AI-powered IAM solutions are vital for organizations to adhere to regulations by consistently and accurately enforcing access controls in the compliance realm. Machine learning algorithms are able to examine access logs and pinpoint possible breaches in compliance, for example, unauthorized entry to confidential information. AI systems are capable of producing thorough audit reports that create precise documentation of access actions, aiding organizations in proving adherence to regulatory guidelines. artificial intelligence is changing Identity and Access Management (IAM) through enhanced features for adaptive authentication, biometric verification, dynamic access controls, insider threat detection, automated identity lifecycle management, and integration of threat intelligence. Its use greatly improves organizations' capacity to safeguard their online assets and guarantee secure entry to vital systems and data. With the ongoing evolution of cyber threats, the use of AI in IAM is predicted to grow, leading to advancements and enhancements in security measures across different sectors[86].

Fig -4: Artificial Intelligence in Identity and Access Management (IAM) Solutions.

14. ARTIFICIAL INTELLIGENCE SOLUTIONS FOR INCIDENT RESPONSE AND MANAGEMENT IN CYBERSECURITY

The use of artificial intelligence (AI) is changing the way incident response and management are done in cybersecurity, as it offers enhanced tools and methods to efficiently and effectively identify, examine, and address cyber threats. Through the utilization of AI, organizations can improve their ability to respond to incidents, quickly identifying and reducing security threats with minimal consequences. This part examines the most recent advancements and developments in AI-based incident response and management solutions. One of the main uses of AI in incident response is in the immediate identification and examination of security incidents. Conventional security systems frequently produce numerous alerts, a significant portion of which are incorrect, causing security teams to be inundated and slowing down their ability to react to real dangers. AI, specifically ML models, is very good at sorting through these alerts to pinpoint real

dangers. ML algorithms can prioritize alerts by analyzing patterns and correlations in security data, allowing security teams to concentrate on the most critical incidents thanks to their severity and potential impact. For instance, methods for anomaly detection can recognize uncommon network traffic or user actions that might suggest a cyber attack, enabling prompt examination and reaction[87-88].

Deep learning (DL) models, which are a part of AI, improve threat detection in incident response even more. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are capable of analyzing vast amounts of data to detect intricate attack patterns and forecast possible security risks. CNNs excel at analyzing network traffic and identifying harmful data, while RNNs specialize in monitoring event sequences to identify active cyber attacks. By utilizing deep learning, incident response systems can enhance their ability to detect threats with greater accuracy and decrease the number of false positives, resulting in more dependable protection against advanced cyber threats. AI is essential in automating the process of examining and addressing security incidents as well. SOAR platforms use AI to automate different parts of incident response for enhanced security orchestration and automation[89]. AI-powered SOAR systems can implement pre-established playbooks to address and resolve detected threats. For instance, an AI system could autonomously separate a device that has been compromised from the network, prohibit malicious IP addresses, and eradicate harmful files. This process speeds up responses and guarantees that dangers are eliminated before they can create major harm. Furthermore, AI has the capability to streamline the gathering and evaluation of forensic data, aiding security teams in promptly grasping the extent and consequences of an incident.

AI improves incident response in threat intelligence by offering immediate insights on new threats. AI algorithms are capable of examining data from different origins, like threat feeds, social media, and dark web forums, in order to detect fresh weaknesses and methods of attack[90-91]. Through combining this threat intelligence with internal security information, AI-powered incident response systems can predict possible attacks and implement proactive measures to reduce risks. For example, if artificial intelligence notices an increase in conversations regarding a particular attack, it can notify security teams to update relevant weaknesses and enhance protections. AI-powered solutions are also vital in improving security teams' awareness of the situation during an incident. AI combines and examines information from various origins to offer a cohesive perspective on the event, aiding in teams' comprehension of its scale and consequences. Machine learning algorithms have the capability to recognize patterns and trends within the data, providing valuable information on the attacker's methods, strategies, and behaviors (TTPs). This extensive awareness of the situation allows security teams to make well-informed decisions and react more efficiently to incidents[90].

Moreover, AI enhances incident response efficiency by lessening the workload on security staff. Investigating and resolving incidents through traditional incident response processes typically involve a substantial amount of manual work. AI streamlines a lot of these tasks, enabling security teams to dedicate their attention to more strategic tasks. For example, chatbots powered by AI can help with the first step of sorting, collecting details of the situation, and offering instant suggestions for controlling and fixing the issue. This automation aids security teams in reacting to incidents with greater speed and effectiveness. AI-powered tools offer important insights for organizations looking to enhance their security stance through post-incident analysis and learning. Machine learning algorithms can recognize patterns and trends that highlight areas for enhancement by analyzing previous incidents and their results. For instance, AI can point out repetitive vulnerabilities or typical attack routes, allowing businesses to tackle these problems and enhance their security measures. AI is capable of producing thorough incident reports, which offer precise documentation of the event and assist organizations in meeting regulatory standards[91].

Furthermore, AI improves organizations' capacity to perform threat-hunting operations. Threat hunting entails actively searching for indicators of malicious actions in the network, rather than depending only on automated notifications. AI-powered threat-hunting platforms utilize machine learning algorithms to scrutinize data and detect signs of compromise (IoCs) that could have been overlooked by conventional security solutions. By constantly acquiring knowledge from fresh data, these systems can adjust to changing threats and expose covert attacks, enhancing the overall efficiency of incident response[92].

15. CONCLUSIONS

This study highlights the important progress and new directions in AI-driven cybersecurity technologies through a thorough analysis of recent research, offering a detailed look at their use and impact. Machine learning (ML), deep learning (DL), natural language processing (NLP), and reinforcement learning (RL) are now recognized as effective resources in different areas of cybersecurity, including threat identification, reaction, network protection, and data security. ML and DL models are highly skilled at recognizing intricate attack patterns and previously unknown vulnerabilities, improving the functionality of intrusion detection systems (IDS) and intrusion prevention systems (IPS). NLP methods are crucial for examining and understanding text data, assisting in threat intelligence, and identifying phishing and social engineering attacks. RL's ability to make decisions in a changing environment allows for the improvement of security strategies in constantly evolving threat scenarios.

The utilization of AI in particular cybersecurity sectors, like threat intelligence platforms, endpoint security, network security, and cloud security, has shown to be very successful. AI-powered threat intelligence platforms offer immediate insights on new threats, while AI-based endpoint security solutions identify and address malware and other harmful actions on personal devices. AI technologies in network security are responsible for monitoring and securing infrastructures, identifying intrusions, and overseeing access controls. The rise of the Internet of Things (IoT) has broadened the reach of AI, ensuring the security of connected devices and intelligent surroundings. The analysis of co-occurrence and clusters in this study provides valuable insights into the primary topics and focuses of AI-driven cybersecurity research. These analyses showcase how different themes in AI cybersecurity are interconnected by examining the frequency and relationships of key terms, emphasizing the multidisciplinary nature of the field. Identifying separate clusters that represent various subfields offers an organized perspective of the research landscape, emphasizing important topics and possible directions for future studies. With the evolution of cyber threats, the importance of AI in cybersecurity is anticipated to grow, leading to advancements and improvements in security measures in different sectors. Future studies should concentrate on filling in the recognized deficiencies, investigating fresh AI uses, and consistently enhancing AI-based solutions to stay up to date with the ever-changing threat environment. Organizations can improve their cybersecurity defenses by maximizing the capabilities of AI, effectively guarding against new threats and protecting their digital assets.

REFERENCES

[1] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature review. International Journal of Advanced Research in Computer and Communication Engineering.
[2] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 564-574.

[3] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 101804.
[4] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.
[5] Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. Computer Science & IT Research Journal, 5(3), 703-724.
[6] Jun, Y., Craig, A., Shafik, W., & Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyberdefense. Wireless communications and mobile computing, 2021, 1-10.
[7] Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. Scientometrics, 121, 1189-1211.
[8] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.
[9] Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.
[10] Yildirim, M. (2021). Artificial intelligence-based solutions for cyber security problems. In artificial intelligence paradigms for smart cyber-physical systems (pp. 68-86). IGI Global.
[11] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1(1), 103-119.
[12] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.
[13] Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531.
[14] Goosen, R., Rontojannis, A., Deutscher, S., Rogg, J., Bohmayr, W., & Mkrtchian, D. (2018). ARTIFICIAL INTELLIGENCE IS A THREAT TO CYBERSECURITY. IT'S ALSO A SOLUTION. Boston Consulting Group (BCG), Tech. Rep.
[15] Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042072). IOP Publishing.
[16] Berghout, T., Benbouzid, M., & Muyeen, S. M. (2022). Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. International Journal of Critical Infrastructure Protection, 38, 100547.
[17] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.
[18] Soni, S., & Bhushan, B. (2019, July). Use of Machine Learning algorithms for designing efficient cyber security solutions. In 2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT) (Vol. 1, pp. 1496-1501). IEEE.
[19] Omar, M. (2022). Machine learning for cybersecurity: Innovative deep learning solutions. Springer Nature.
[20] Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. European Journal of Technology, 7(2), 1-14.
[21] Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), 1-38.
[22] Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.
[23] Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 212, 109032.
[24] Omar, M. (2022). Machine learning for cybersecurity: Innovative deep learning solutions. Springer Nature.
[25] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371-390). IEEE.
[26] Imamverdiyev, Y. N., & Abdullayeva, F. J. (2020). Deep learning in cybersecurity: Challenges and approaches. International Journal of Cyber Warfare and Terrorism (IJCWT), 10(2), 82-105.
[27] Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), 154.

[28] Kaushik, D., Garg, M., Gupta, A., & Pramanik, S. (2022). Application of machine learning and deep learning in cybersecurity: An innovative approach. In An Interdisciplinary Approach to Modern Network Security (pp. 89-109). CRC Press.

[29] Lago, C., Romón, R., López, I. P., Urquijo, B. S., Tellaeche, A., & Bringas, P. G. (2021). Deep learning applications on cybersecurity. In Hybrid Artificial Intelligent Systems: 16th International Conference, HAIS 2021, Bilbao, Spain, September 22–24, 2021, Proceedings 16 (pp. 611-621). Springer International Publishing.

[30] Georgescu, T. M. (2020). Natural language processing model for automatic analysis of cybersecurity-related documents. Symmetry, 12(3), 354.

[31] Arjunan, T. Detecting Anomalies and Intrusions in Unstructured Cybersecurity Data Using Natural Language Processing.

[32] Singh, K., Grover, S. S., & Kumar, R. K. (2022, June). Cyber security vulnerability detection using natural language processing. In 2022 IEEE World AI IoT Congress (AIIoT) (pp. 174-178). IEEE.

[33] Frank, E., Oluwaseyi, J., & Olaoye, G. (2024). Introduction to natural language processing (NLP) in cybersecurity.

[34] Georgescu, T. M., Iancu, B., Zamfiroiu, A., Doinea, M., Boja, C. E., & Cartas, C. (2021). A survey on named entity recognition solutions applied for cybersecurity-related text processing. In Proceedings of Fifth International Congress on Information and Communication Technology: ICICT 2020, London, Volume 2 (pp. 316-325). Springer Singapore.

[35] Sharma, S., & Arjunan, T. (2023). Natural Language Processing for Detecting Anomalies and Intrusions in Unstructured Cybersecurity Data. International Journal of Information and Cybersecurity, 7(12), 1-24.

[36] Marinho, R., & Holanda, R. (2023). Automated emerging cyber threat identification and profiling based on natural language processing. IEEE Access.

[37] Ukwen, D. O., & Karabatak, M. (2021, June). Review of NLP-based systems in digital forensics and cybersecurity. In 2021 9th International symposium on digital forensics and security (ISDFS) (pp. 1-9). IEEE.

[38] Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779-3795.

[39] Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. Information Systems Frontiers, 25(2), 589-611.

[40] Adawadkar, A. M. K., & Kulkarni, N. (2022). Cyber-security and reinforcement learning—A brief survey. Engineering Applications of Artificial Intelligence, 114, 105116.

[41] Sewak, M., Sahay, S. K., & Rathore, H. (2021, October). Deep reinforcement learning for cybersecurity threat detection and protection: A review. In International Conference On Secure Knowledge Management In Artificial Intelligence Era (pp. 51-72). Cham: Springer International Publishing.

[42] Cengiz, E., & Gök, M. (2023). Reinforcement learning applications in cyber security: A review. Sakarya University Journal of Science, 27(2), 481-503.

[43] Li, C., & Qiu, M. (2019). Reinforcement learning for cyber-physical systems: with cybersecurity case studies. Chapman and Hall/CRC.

[44] Yu, Y., Yang, W., Ding, W., & Zhou, J. (2023). Reinforcement learning solution for cyber-physical systems security against replay attacks. IEEE Transactions on Information Forensics and Security.

[45] Cam, H. (2020, April). Cyber resilience using autonomous agents and reinforcement learning. In Artificial intelligence and machine learning for multi-domain operations applications II (Vol. 11413, pp. 219-234). SPIE.

[46] Gupta, S., Sabitha, A. S., & Punhani, R. (2019). Cyber security threat intelligence using data mining techniques and artificial intelligence. Int. J. Recent Technol. Eng, 8, 6133-6140.

[47] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.

[48] Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 135-154.

[49] Tetaly, M., & Kulkarni, P. (2022, October). Artificial intelligence in cyber security–A threat or a solution. In AIP Conference Proceedings (Vol. 2519, No. 1). AIP Publishing.

[50] Goosen, R., Rontojannis, A., Deutscher, S., Rogg, J., Bohmayr, W., & Mkrtchian, D. (2018). ARTIFICIAL INTELLIGENCE IS A THREAT TO CYBERSECURITY. IT'S ALSO A SOLUTION. Boston Consulting Group (BCG), Tech. Rep.

[51] Akinsola, J. E. T., Akinseinde, S., Kalesanwo, O., Adeagbo, M., Oladapo, K., Awoseyi, A., ... & Heimgartner, R. (2021). Application of artificial intelligence in user interfaces design for cyber security threat modeling (pp. 1-28). IntechOpen.
[52] Veiga, A. P. (2018). Applications of artificial intelligence to network security. arXiv preprint arXiv:1803.09992.
[53] Suárez, L., Espes, D., Le Parc, P., Cuppens, F., Bertin, P., & Phan, C. T. (2018, November). Enhancing network slice security via Artificial Intelligence: Challenges and solutions. In Conférence C&ESAR 2018.
[54] Haider, N., Baig, M. Z., & Imran, M. (2020). Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. arXiv preprint arXiv:2007.04490.
[55] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.
[56] Yoo, S. J. (2018). Study on improving endpoint security technology. Convergence Security Journal, 18(3), 19-25.
[57] Maddireddy, B. R., & Maddireddy, B. R. (2021). Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications. Revista Espanola de Documentacion Cientifica, 15(4), 154-164.
[58] Singh, S., Karimipour, H., HaddadPajouh, H., & Dehghantanha, A. (2020). Artificial intelligence and security of industrial control systems. Handbook of Big Data Privacy, 121-164.
[59] Arfeen, A., Ahmed, S., Khan, M. A., & Jafri, S. F. A. (2021, November). Endpoint detection & response: A malware identification solution. In 2021 International Conference on Cyber Warfare and Security (ICCWS) (pp. 1-8). IEEE.
[60] Islam, M. A. (2023). Application of artificial intelligence and machine learning in security operations center. Issues in Information Systems, 24(4).
[61] Turgay, M. (2023). The impact of artificial intelligence on cybersecurity. Вестник Науки и Творчества, (3 (85)), 51-53.
[62] Addo, A., Centhala, S., & Shanmugam, M. (2020). Artificial intelligence for security. Business Expert Press.
[63] Yoo, S. J. (2018). Study on improving endpoint security technology. Convergence Security Journal, 18(3), 19-25.
[64] Maddireddy, B. R., & Maddireddy, B. R. (2021). Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications. Revista Espanola de Documentacion Cientifica, 15(4), 154-164.
[65] Mautone, R. M. A., & Priest, C. S. (2023). U.S. Patent Application No. 18/009,926.
[66] Turgay, M. (2023). The impact of artificial intelligence on cybersecurity. Вестник Науки и Творчества, (3 (85)), 51-53.
[67] Jenkinson, T., Sansom, D., Heinemeyer, M., & Stockdale, J. (2022). U.S. Patent No. 11,477,219. Washington, DC: U.S. Patent and Trademark Office.
[68] Addo, A., Centhala, S., & Shanmugam, M. (2020). Artificial intelligence for security. Business Expert Press.
[69] Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Authorization, and Access Control within Cloud-Based Systems (January 25, 2024).
[70] Mohammed, I. A. (2021). Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored and Controlled. International Journal of Creative Research Thoughts (IJCRT), ISSN, 2320-2882.
[71] Adenola, V. (2023). Artificial intelligence based access management system. East Carolina University.
[72] Aboukadri, S., Ouaddah, A., & Mezrioui, A. (2024). Machine Learning in Identity and Access Management Systems: Survey and Deep Dive. Computers & Security, 103729.
[73] Singh, C., Thakkar, R., & Warraich, J. (2023). IAM identity Access Management—importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research, 8(4), 30-38.
[74] Azhar, I. (2018). A literature review on the application of AI to Identity Access Management. Ishaq Azhar Mohammed," A literature review on the application of AI to Identity Access Management", International Journal of Emerging Technologies and Innovative Research (www. jetir. org| UGC and issn Approved), ISSN, 2349-5162.
[75] Maciel, L. R., & Dhakal, V. (2020). 'Applying AI concepts for identity and access management in cloud environments. NYU Tandon School Eng., New York Univ., Tech. Rep.
[76] Masawi, A., & Matthee, M. (2023, August). Guidelines for the Adoption of Artificial Intelligence in Identity and Access Management Within the Finan

[77] cial Services Sector. In International conference on WorldS4 (pp. 111-127). Singapore: Springer Nature Singapore.
[78] Hassan, S. K., & Ibrahim, A. (2023). The role of artificial intelligence in cyber security and incident response. International Journal for Electronic Crime Investigation, 7(2).
[79] Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), 1720-1736.
[80] Trifonov, R., Manolov, S., Tsochev, G., & Pavlova, G. (2019). Automation of cyber security incident handling through artificial intelligence methods. WSEAS Transactions on Computers, 18, 274-280.
[81] Nilă, C., Apostol, I., & Patriciu, V. (2020, June). Machine learning approach to quick incident response. In 2020 13th International Conference on Communications (COMM) (pp. 291-296). IEEE.
[82] Jain, J. (2021). Artificial intelligence in the cyber security environment. Artificial Intelligence and Data Mining Approaches in Security Frameworks, 101-117.
[83] Uzoma, J., Falana, O., Obunadike, C., Oloyede, K., & Obunadike, E. (2023). Using artificial intelligence for automated incidence response in cybersecurity. International Journal of Information Technology (IJIT), 1(4).
[84] Simonovich, L. (2020, November). Cyber Security Incident Response in the Utility Sector. In Abu Dhabi International Petroleum Exhibition and Conference (p. D021S042R003). SPE.
[85] Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches To Cloud Security Incident Management. Chelonian Research Foundation, 15(2), 1-10.
[86] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.
[87] Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex & Intelligent Systems, 8(2), 1763-1780.
[88] Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 143-154.
[89] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254.
[90] Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.
[91] Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEE Access, 10, 93104-93139.
[92] Aloqaily, M., Kanhere, S., Bellavista, P., & Nogueira, M. (2022). Special issue on cybersecurity management in the era of AI. Journal of Network and Systems Management, 30(3), 39.

DECLARATIONS

- Funding: No funding was received.
- Conflicts of interest/Competing interests: No conflict of interest.
- Availability of data and material: Not applicable.
- Code availability: Not applicable.
- Acknowledgments: Not Applicable.