ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ALGORITHMS ARE USED TO DETECT AND PREVENT CYBER THREATS AS WELL AS THEIR POTENTIAL IMPACT ON THE FUTURE OF CYBERSECURITY PRACTICES.

Md Al Amin

St. Francis College MS in Information Technology

ABSTRACT

As many devices connect to the internet and people save more information on the cloud and increase their usage of digital communication, the threat level on the information sphere has increased significantly. With the increase of device connectivity and use of money transactions cyber threats have become more sophisticated than ever. Conventional discrete security policies are ineffective to address the behavioral and constantly changing nature of today's cybersecurity threats such as zero-day exploits, APTs or ransomware. In this light, AI and ML are considered strategic technologies, which define cutting-edge, intelligent, adaptive as well as scalable cybersecurity solutions.

AI and ML are very effective in the processing of big data from a variety of sources including the networks traffic, logs, and endpoints behavior to detect, analyze and contain threats in real-time. In contrast, these technologies update their algorithms over time depending on new information and are therefore capable of addressing hitherto unseen vulnerabilities. Behavioral analytic system, Intrusion detection and prevention system is the most used technologies to detect, analyze and prevent cyber threats. For example, ML can pick out 'anomalous user activity' as a sign of insider threats or stolen login credentials while AI-based systems can stop malicious actions by analyzing network traffic in milliseconds.

In addition, through AI and ML the threats are analyzed with a focus on the risk in the future based on the previous exposition. That proactive capability alone cuts response time so organizations can take more effective measures to enhance security and mitigate cyber threats to growing connectivity and increasing security on digital transactions. that organizations can do a better job of managing risk. Another way that AI helps in the incident management is making automated response mechanisms for such situations, and a system can effectively counter spontaneous threats than coming in physically. Even though they still present a number of difficulties, these technologies have certain special benefits. The use of AI by cyber adversaries by means of data poisoning attacks, algorithm shifting attack as well as adversarial AI generate new forms of risks. The criticisms regarding data privacy, bias and self-accountability of AI regarding increased cybersecurity also need to be settled.

All in all, the use of AI and ML in cybersecurity is a game changer in terms of the identification, management, and prevention of threats. These technologies bring in the flexibility and wisdom to protect the current information territory from emerging threats. However, for their deployment to yield these benefits, solid frameworks should support them to reduce risk and enhance reliability. AI and ML will remain essential tools as the information sphere develops further, in order to protect the information space.

DOI: 10.5121/ijcsit.2025.17101

KEYWORDS

AI, Defensive AI, Zero-Day Threats, Threat Mitigation, Behavioral Analysis, Compromised Accounts, Real-Time Monitoring, Dynamic Analysis.

1. INTRODUCTION

Information space has grown rapidly due to smart devices, cloud computing, and modern developments in communication technologies in the past few years, which makes systems extremely vulnerable to cyber threats. The ongoing growth of digital commerce and the internet of things has made people more subject to cyberattacks. The vulnerabilities about the main critical systems are gradually increasing concerns as devices get intertwined and data rapidly shared between one platform to another. It has been found that as the number of connected devices and networks rises, there has been tremendous pressure on conventional security models to contain the number and level of threat, including ransomware, phishing attacks, APTs and zero-day attacks [1], [2]. This has made organizations vulnerable to more threats hence necessitating change in the way security is done.

Conventional security models are largely conceptual, and act based on certain rules and suggested countermeasures regarding cyber threats. This kind of model worked well in previous years and earlier times when threats were calculated and automated, not to mention constant. These conventional methods involve slow reactions most of the time. It provides attackers with ample time to penetrate into networks wreaking havoc but before adequate counter measures are deployed. The inherent limitation of traditional approaches is that they do not incorporate a means of generating new rules when the organization confronts novel threats it has never faced before.

However, recent developments in machine learning (ML) and artificial intelligence (AI) offer an innovative solution for all of the issues associated with standard cybersecurity frameworks. AI and ML have given the cybersecurity systems a pl atform to be intelligent and dynamic in their approach to threats and safeguards them against impending threats. These technologies use big data techniques to analyze normal behavior within the systems and networks they protect and thus be able to spot such changes and anomalies as a sign of an attack. The speed at which AI and ML can sift through vast amounts of data makes them superior to human analysts and analysts' traditional tools, when it comes to identifying new, quite often unique threats that may otherwise go unnoticed in the sheer volume of network traffic, system logs, and endpoint interactions[3].

The most beneficial aspect of AI and ML in cybersecurity is the capacity to recognize the deviations from the standard activity patterns. Of all AI categories, behavioral analytics has been found to be rather effective in detecting lateral movements and insider threats. By studying user's behavioral pattern or daily routine, then an AI system can identify what is a typical trace for a particular user or group of users. When activity is clearly outside of this norm— For example, if an individual is pulling a file at 3 a.m., or downloading tremendous levels of information—AI models can quickly identify this as potentially problematic. This gives a strong mechanism to detect the illicit activities that occur in the network before they cause severe harm that would be fatal in case they are a breach.

Along the same line, AI and ML are applied to protect it from invasions through techniques known as Intrusion Detection and Prevention Systems (IDPS). These systems receive and analyze traffic in a real-time basis and thereby have the capability to detect any form of unlikely malicious activities on the network. Structurally, AI is the only viable approach since it is capable of continually

incrementally learning from the traffic at hand and detecting and mitigating threats that would otherwise take human analysts a lifetime to even identify.

Apart from the behavioral assessment and intrusion assessment, AI and ML also feature in the prediction section of threat intelligence. In the past, threat intelligence involved analysts analyzing and use their skill and knowledge of the attack. This approach can be useful, but it is limited when the next threat that has not been discovered is being pushed. Because predictive threat intelligence thus leverages AI and ML, in that it uses data mining, threat repositories and historical attacks to provide systems a way to forecast the next types of threats likely to occur, this dynamic is altered. Machine learning algorithms used can detect patterns on how attackers are planning on launching their attacks and facilitating organizations' ability to protect against new dangers. This predictive capability enables the security teams to take pre-emptive measures, apply security fixes, and incur security mechanisms to prevent exploit of the vulnerability thus limiting the attackers' window.

In addition, with AI and ML, there is automation, which is vital in dealing with incident response, and risk management functions. Reactive measures taken by the hands will likely take time and therefore the attackers will have a field day making more advances. As AI mechanisms help identify, analyze and respond to incidents, the overall response time and the impact of attack can be minimized greatly. This puts the attack out quickly in addition to letting data security specialists avoid lower-level work by handling critical tasks such as the identification of the root cause of the attack and work on strengthening the company's defenses.

However, AI and ML have become common in cybersecurity, though there is a drawback that comes with it. While these technologies are as strong as they are, they do not exempt talent cybercriminals from influencing them. The exploitation vulnerabilities of data and algorithm are another conducing factor to AI in cybersecurity, and the general risk is data poisoning, where a perpetrator feeds an AI system with a wrong or detrimental input data set. Such an attack might involve poisoning the data on which the identified AI models depend and thus deceive the system into ignoring real threats or otherwise labeling potentially dangerous activities as harmless[5]. Data poisoning attacks are dangerous insofar as they go, and if they are not detected sooner than later; hence there should be a need to put in place measures that can protect AI models from such attacks that compromise the security and functionality of these models.

Another issue that has also been addressed is the vulnerability to AI being launched an attack on other AI. It is however worthy of noting that just as the concept of AI and ML has continued to develop so has the approach taken by hackers to subvert the same. For example, adversarial machine learning procedures can always modify the inherent models of the AI systems just to be less precise and also to generate a large number of false positive alerts to the security teams. These attacks can put a lot of pressure on AI security solutions, and in fact, threaten an organization's overall security position.

2. BACKGROUND AND RELATED WORK

Prior work in AI and ML in cybersecurity is concerned with improving the ways of detecting, preventing, and managing cyber threats. IDS is one of the specific topics that must be addressed, where various methods namely supervised, unsupervised and reinforcement learning are employed in looking for signs of mischief in a network. This is more effective than the traditional approach of threat identification, which is time-consuming. Security activity monitoring techniques track the activity of users with the intention of detecting insiders and accounts that have been compromised by comparing present activity with typical activity. It is also used in ransomware detection by analyzing

file behavior, system transactions and network Unfamiliarity patterns to indicate a ransomware incident. Further, ML-powered threat intelligence patterns the potential threats and strengthens preventive solutions in cybersecurity. The implementation of XAI seeks the enhancement of the trust relationship that exists between AI and human analysts in an organization. However, there are still

OBJECTIVES, such as adversarial attacks counter and data biases, that can be considered as the promising directions for developing AI- based cybersecurity solutions further.

2.1. AI's role in behavioral analysis as applied to cybersecurity.

This work explores how AI-backed behavioral analyze s tools work to monitor and alert on insider threats, compromised accounts, and unauthorized access. The historical usage data, behavior patterns, baseline, and dynamic analysis for real-time threats are all highly important in this method.

These inside jobs are becoming more technical to pull off and with the use of compromised accounts, intelligent behavioral analysis tools from AI are critical in cybersecurity. These tools use gathered data about past usage and analyze current behavior and activity to produce deviations from normal and uncover danger before they occur.

In a financial institution, the workers can get under one roof, a consolidated database that has details of their respective clients. For protection from malice and account abuse, a behavioral analytics system based on AI technology is used [4]. The system monitors the activities of the employees so as to determine the normal behavior of such employees. For instance, it learns an employee's log-in times, their normal interaction with the files and their overall usage of data. This provides the system with a baseline to determine what is active or normal to the case at hand, and what is suspicious.

There is a day when the system registers suspicious use of an employee's account. The login occurs at 2:00 AM from a foreign IP address which is very peculiar from the normal usual flow. The account starts to gain access to other administrative files such as the confidential ones the user has never had a chance to open. In addition, a huge number of files are downloaded within a short time exceeding the amount the employee normally downloads, of over 200MB.

These irregularities are quickly detected by the AI system and prompt an automatic corresponding response. Immediately, the cybersecurity team gets an alert, access to those sensitive files becomes locked to avoid further leakage and an email is generated to the employee to confirm the worrying log in.

When looking carefully, the cybersecurity team finds out that the account was affected by a phishing attack. The attacker was interested in exfiltrating data, but due to the effective AI system, it was prevented on the spot.

This case is a clear example of how great value AI is to security systems, specifically behavioral analysis. This set of tools uses historical data and real-time monitoring to analyze risks and immediately respond to threats, reducing consequences and improving organizational defense in general.

2.2. Intrusion detection system IDS using; Machine learning is used here for detecting the intrusion.

Explains how ML algorithms can improve intrusion detection in more detail with reference to the ways in which it improves upon the analysis of traffic and patterns of such networks through algorithms. Supervised, unsupervised, and reinforcement learning methods of building IDS models are also discussed.

The traditional IDS has changed with the help of ML because the systems have learned how to analyze the traffic and detect new threats. Most of the existing IDS work under the traditional approach that depends on pattern matching technology and therefore they lack capability to detect new variants of known attacks or previously unseen attacks known as zero-day threats [2]. These are handled by ML, whereby algorithms are used to probe through the network traffic in order to deduce abnormalities.

An example of practical usage can be observed in the case of a multinational company that decided to install an ML based IDS, in order to regulate the company's network. The system learns the normal traffic and the traffic which is malicious through prior labelled data such as Random Forest or SVM. These algorithms gain capability to differentiate between normal and anomalous traffic depending on characteristics such as size of packet, type of protocol, and source/destination IP addresses. In live traffic, the system works in parallel with the learned data pattern and immediately raises an alert for any suspicious activity. For instance, it detects a Distributed Denial of Service (DDoS) through analyzing a pattern of repeated traffic from servers that are most likely to result in a malware infestation so that it can isolate servers that are under attack.

Besides supervised learning the IDS utilizes unsupervised learning techniques, for example clustering (K-Means or DBSCAN; which identify new threats that the system has not encountered before. Unlike the supervised methods, these algorithms classify traffic behaviors and mark anything that deviates from the grouped pattern as an intrusion. For example, an insider threat might be identified when an employee downloads massive quantities of data to an external server at a time when such action is rare. This is a typical system event, and the security team is informed of the change.

The coexistence of supervised and unsupervised learning facilitates the implementation of ML-based IDS in both a known and unknown level threat. These systems learn new patterns of attacks, can differentiate the real threats from noise, and minimize the number of false alarms. Consequently, IDS, powered by ML, enhances network security profoundly, providing organizations with a leading defense against constantly developing threats.

2.3. Threat Intelligence Using Machine Learning

Machine learning threat intelligence allows organizations to leverage past experience by identifying potential threats and eliminating them. Learning from past attacks, weaknesses, and dangerous actions, Unsafe areas explain new threats and provide recommendations for protective cybersecurity actions. It is this approach that turns conventional disruptive measures to positive action, thereby using predictive analysis to counter threats.

An autonomous organization adopted an advanced guard solution of Threat Intelligence through the use of Artificial Intelligence. The platform initially processed quantitative data such as previous

campaigns, malware type, attack patterns, vectors and external qualitative data that encompass the dark web activity, reports of newly discovered bugs. From this, the system extracted information of unauthorized discussions on hacker forums, regarding a recently developed ransomware, which is aimed at enterprise cloud storage solutions. Based on this understanding, the system related this information with data from previous ransomware attacks to gauge that the ransomware would leverage unsolved vulnerabilities in cloud service APIs.

The data mining showed working results for the cybersecurity team as it leveraged the importance of patching the several cloud API's considered high risk. The system also documented signs of the ransomware propagation including large numbers of files encrypted and large volumes of CPU usage.

The use of predictive analysis allowed for details regarding an expected schedule of the attack to be identified in advance so the organization could construct defenses appropriately.

Several weeks later, the platform used to monitor the organization's movements noticed some illicit operation in the cloud servers, comparable to the forecast of the ransomware. Notification was raised and all the related systems were quarantined to ensure that the ransomware did not lock crucial data. The predictive intelligence helped make sure that potential vulnerabilities in the organization were protected to prevent an attack.

This example shows how integrating ML-based threat intelligence into cybersecurity improves the process by learning from past data and subsequently predicting possible risks in future. This proactive approach enables the organizations to avoid risks, be prepared for the worst and guaranty quick response to the new emerging threats.

2.4. Adversarial Attacks in AI Security Systems

They take advantage of the defects in deep learning AI and are a major threat to AI security systems. These attacks are data poisoning, by which the training data is contaminated to poison the model, and evasion attacks for which the adversaries slightly alter the inputs to get past the detectors. They both expose the weakness of AI models and also stress the importance of a strong countermeasure against various forms of sabotage. For instance, let us consider an intelligent anti-virus system designed to smooth through different files, driving how dangerous or safe they are, relying on metadata and file actions. The risk of a more invasive type of attack called data poisoning is that a hacker can feed the system with wrong examples of the training data set. Such contaminated samples could involve inserting harmless appearing files that could have negative attributes masked from the model. Consequently, the system loses its efficiency, and more malwares can escape its notice during the real-time running of the program. Of course, in an evasion attack the hacker could create malware precisely to avoid detection by the given anti-virus. It alters all aspects of the malware's code slightly—changes that are invisible even to human researchers—and guarantees that the AI model will classify it as benign. This particular strategy of attack takes advantage of the model's inability to generalize and depends on a small number of parameters.

There exists a need for protection against adversarial attacks. Techniques such as Adversarial training, where during training models are exposed to adversarial examples increase robustness. Other approaches are: Adversarial decision trees, Anomaly detection system which alerts for suspicious behavior, Defensive distillation which reduces the effect of small input perturbation. Moreover, it is beneficial to explain which decisions an AI model has made, as well as which areas can be vulnerable, with the help of explainable AI methods.

The present work presents the issues of the adversarial attack and asks questions about the possibility of exposing different AI methods to an attempt at manipulation in the present analysis. Defending the AI models against adversarial interference continues to remain a critical challenge particularly as hackers become smarter in their operations.

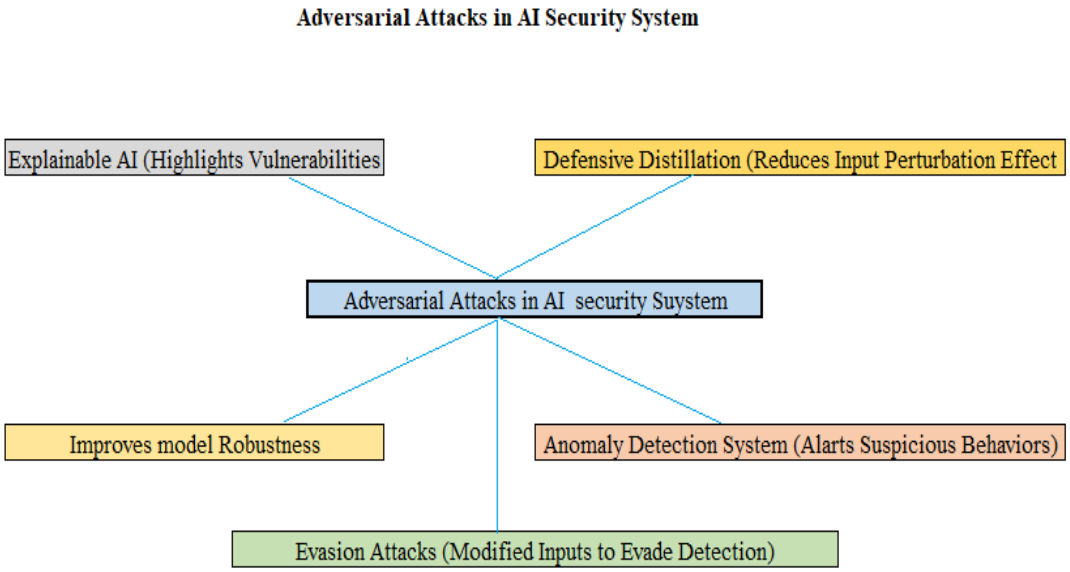


Figure-1: Adversarial Attacks in AI Security System

3. HANDLING REAL-LIFE INCIDENTS USING AI

Risk management of actual cyber occurrences with the help of artificial intelligence has changed the speed of the threat's neutralization. Since the system employs the use of AI, the process of identifying, analyzing and implementing countermeasures for security threats takes a relatively short period than it would take when done manually. Technologies such as SIEM use Artificial Intelligence for network monitoring as well as threat identification and management with necessary responses.

In real life, an ML integrated to the SIEM platform can process large volumes of data from firewalls, IDS and endpoints, among other sources. For instance, whenever a SIEM system identifies multiple geographical locations attempting to log in within a few minutes – as is typical of a credential-stuffing attack – the AI algorithms analyze the situation in real-time. By assessing the contextual information of the compromised systems, user activity profile and intelligence feeds they assess the likelihood of active threat.

It then launches automated playbooks, a pre-set response framework meant to counter given risk factors. Possibly, the steps of the playbook may be, for example, the blockage of the account, enabling of the MFA for all accounts and blocking of the IP-addresses at Firewall. Since decision algorithms are built on AI, these actions are prioritized according to threat level and how important the compromised systems are.

However, apart from simple responses, an AI system also provides rich context for each incident to the cybersecurity team and identifies the root cause and system that was impacted. This allows the

security teams to work on high priority incidents and provide informed decisions. For instance, if the SIEM identifies patterns that suggest phishing attacks against employees, it can send a message to notify users and adjust the firm's spam filters to filter out such emails.

The use of AI in managing incidents and executing decisions real-time thereby strengthens an organization against cyber threats. They make certain that the actual real-life cyber security incidents are handled effectively with less response time, repetitive tasks, and more insights.

4. AI IN CLOUD SECURITY

Cloud security is an area where artificial intelligence is critical in solving issues that are specific to cloud environments, beginning with scalability and dynamic systems and including shared responsibility models. AI is also used in high-advanced security for data and individuals' identities, as well as continuous threats detection in cloud systems.

Cloud computing is especially exposed to unauthorized entry, data violation, and misconfigurations. These problems are solved by AI handling the constant observation of users' behavior and their access to the program. For example, in analyzing login activities, geo location and device information the AI models is able to detect inconsistencies. Let us consider a case where a user tries to log into the cloud application from an unknown or unfamiliar location or device, then the system will alert and may require entering more facts, for instance, MFA.

Another aspect where AI enhances the cloud security aspects is Data protection. Machine learning and artificial intelligence depend upon encryption management, anomaly detection and automated compliance checks apart from safeguarding the cloud data [6]. For example, if an AI model identifies abnormally frequent data traffic such as the downloading of many files from a cloud storage service, then the model can immediately limit the access, notify the security team and slow down the data leakage.

AI can learn a lot about threat detection in cloud environments due to the capability of incorporating big data to analyze them in real-time. The implemented machine learning routines can detect previously unnoticed exploits, including zero-day malware, based on the patterns akin to the dangerous behavior. For instance, in a cloud infrastructure, AI systems may find a distributed denial of service (DDoS) attack since the traffic origin of an attack differs from the expected from a single and multiple source; the system automatically countermeasures when it scales up the resources to handle the load or blacklists Ip addresses that are considered malicious.

There is also misconfiguration which is one of the biggest threats within cloud environments that is solved by AI. AI-assisted technologies look for vulnerabilities, for example, overprivileged access settings in networks and also offer AI-based solutions to fix them. Using AI, organizations can guarantee the constant fulfillment of security policies, make timely prevention of threats, and provide the security of cloud infrastructures.

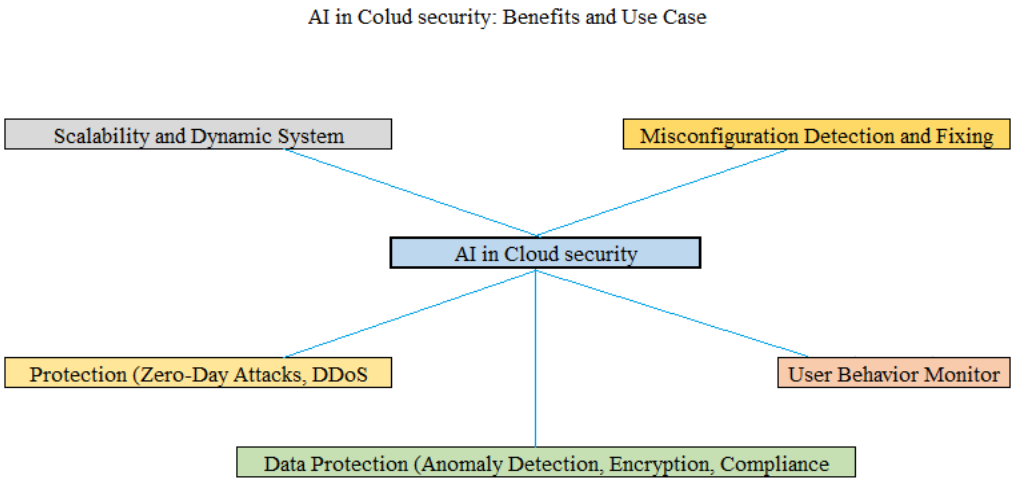


Figure-2: AI in cloud security- Benefits and Use Case

5. AI FOR DETECTION AND PREVENTION OF RANSOMWARE

It is now impossible to walk through the corridors of the modern organization without accidents with AI and ML – these are indispensable assets that help prevent ransom attacks and analyze files, monitor transactions on a network. The current forms of ransomware protection are based on the signatures for the threats and the methods have their problem when facing the new ransomware variants or using the techniques for the first time. The above models have limitations due to the inability of rule-based systems to identify new suspicious patterns and anomalies in real time; this is however overcome by AI-driven models.

AI models help pattern and observe the behavior of files and access to them and such to identify ransomware activity. For instance, ransomware may crypt hundreds and thousands of files in minutes, such a rate is easily captured by monitoring file modifications with AI. When something like unusual file encryption activity is detected, the AI-based systems immediately generate alarms and can also halt the process. Likewise, if a system starts writing files in encrypted form with extensions that are characteristic of ransomware, the AI alerts that the system has been infiltrated.

AI continues to perform well in network activity analysis which is paramount in combating ransomware. For instance, ransomware interacts with command and control (C2) servers to get instructions or to transfer encrypted keys. Using the ML algorithms, AI is able to identify such communication patterns as outgoing traffic or connection with IPs and isolate the affected devices. An example would be filtering domains out that are found in threat intelligence lists which are related to ransomware traffic[7].
Further, system transaction monitoring is another part in which AI boosts ransomware protection. The AI models can set up and monitor regular patterns of system functioning and can detect abnormalities like granting unpopular user permissions, process that tries to access forbidden directories. These indicators may be deployed in advance to prepare the ground for ransomware attack and, hence, they may trigger instant containment actions.

For instance, a financial institution had applied an AI-based ransomware detection capability which enabled it to mitigate an attack at its infancy. The tool considered a workstation whose encryption activity was different from the average detected connections to a domain with known malicious

content. The individually-set workstation was isolated by the system and the connection was severed before all the data could be encrypted and lost.

When applied to file behavior analysis or network monitoring, as well as scrutiny of system transactions, AI performs a 360-degree assessment of ransomware threats. The important fact of its capability to learn new ransomware variants protects adequately from these growing complex threats.

6. HUMAN – AI PARTNERSHIP IN THE COURSE OF CYBERSECURITY

One of the most important trends in current security is the symbiosis of artificial intelligence and human analysts who are capable of cooperating as a single team to handle modern threats. Artificial Intelligence in this case is not expected to supplant the role of the analyst but enhance him or her by enhancing ability to process data that can be used to identify, respond or even prevent emerging threats. This collaboration maximizes the strengths of both humans and machines: the capabilities of the computer, in terms of the speed and optimization of AI and the problem solving and interpretational abilities of human beings.

AI systems work well with big data processing, real-time analysis of large datasets and finding correlations while humans may not while working on them. For instance, in an APT case, an algorithmic system might identify suspicious horizontal mobility within a network or find new forms of malware. Nevertheless, these alerts are frequently detailed and need human input for verification, analysis, and assessment of the resulting actions. There is a way for the analysts to find out more about the context of the activity as something which might be risky or suspicious in the given environment, including the organizational knowledge and business goals as well as threat intelligence. In this partnership, XAI intervenes as it helps in the improvement of trust and system usability. Classical approaches in AI called ‘black box’ do not give insight into how they make decisions and that creates skepticism among analysts. XAI is relevant in dealing with this issue since the model seeks to explain the actions or recommendations of an AI system. For instance, an XAI-based cybersecurity system can inform an analyst that an alert was generated because user ‘A’ opened files on server ‘B’ that are normally accessed on server ‘C’ after three incorrect login attempts. Of course, such transparency makes it easier for the analysts to determine why certain decisions were made by the AI and this leads to better responses to be given with more confidence in the machine.

Furthermore, when humans and AI work together, the process is always improving. AI systems can be valued for responding to a particular situation by telling analysts either that something might be considered a false positive or, conversely, that something might have been missed as a threat. Such an iterative process makes it possible to develop AI in parallel with the emergence of new cyber threats and still maintain connection and compliance with man authority and knowledge. Thus, people and AI enhance a more robust and flexible cybersecurity model for countering new or continually emerging threats by automating cybersecurity processes while making important decisions.

7. METHODOLOGY

The methodologies in this research focus on the impact of AI and ML regarding the dynamic practice of cybersecurity, which then results in quick, precise, and ever-evolving actions against threats.

Altogether, every methodology provides an association for threat discovery, analysis, and strategy, developing a comprehensive defense mechanism for organizations.

7.1. Analysis of Behavior in Cybersecurity

Behavioral analysis with reference to Artificial Intelligence involves tracking of user activities and identification of any form of deviation from the normal activity through benchmarking of the real time activity. Described below are usage histories to which normal patterns such as login time and file access routines are computed on. Electronic control in AI systems constantly checks for instances of activity such as foreign IP logins or even large numbers of files downloaded. For example, a financial institution's AI system detected suspicious behavior when an employee's account was accessed at 2: from a foreign IP and as such immediate mitigation measures were put in place at 00 AM. This methodology focuses on the strength of how insiders' threats and compromised accounts can be identified and responded to with the aid of AI backed tools.

7.2. IDS with Machine Learning Approach

MLS extensible IDS employs the use of logics of artificial intelligence in dealing with traffic in search of threats. In supervised learning, Random Forest and SVM train traffic data sets then separate it into traffic that is normal and traffic that is malicious. Other techniques like K-MeANS or DBSCAN in unsupervised learning are grouping the traffic patterns so as to identify emergent type of anomaly, for instance the zero-day threats. An example in real life involves using packet size and frequency to detect Distributed Denial of Service (DDoS). This even orientation makes IDS flexible to focus on both existing and emerging threats to ensure it is very effective at stopping modern, advanced cyber threats.

7.3. Managing Incidents with the help of AI incorporated SIEM

SIEM solutions based on artificial intelligence collect information from firewalls, Intrusion Detection Systems, and endpoints to evaluate threats in real time. AI compares login information, activity, and intelligence feed to identify cases like credential-stuffing attacks. Countermeasures procedural 'scripts,' which are carried out automatically, include account deactivation, enforcement of MFA for the accounts concerned, and quarantining of the infected computers. Furthermore, AI offers detailed incident content, which helps teams to concentrate on the most important problems and study the sources of the occurrences. For instance, AI remains capable of adapting spam prevention and informing the relevant users of the phishing attempts. This approach reduces response time and also improves the decision-making process.

7.4. The Positives of Risk Management through Artificial Intelligence

Risk management is revolutionized by AI because of the automation of threat recognition, threat assessment, and deployment of counter measures. Supreme AI systems work with large data sets to eliminate threats within a short time. Risk management decisions are heeded according to the threat level and the significance of the system affected. Measures of flexibility like enhancing filters or putting out alerts guarantee the optimum protection from new threats. For example, AI can prevent dummy IP addresses from connecting and can freeze user accounts during an attack. It enhances the organization's capabilities to handle incidents and increase effectiveness in case of an incident occurrence.

7.5. Case-Based Analysis

Real life examples support the approaches used confirming the fact that AI is reasonable in each case. For example, an IDS that relied on artificial intelligence identified the insider threat that put in place

multiple huge downloads that are unauthorized. Likewise, an AI supporting SIEM was able to disrupt a phishing campaign by studying users behavior and adapting counter measures. These examples clearly depict endow AI for monitoring different types of threats with easy efficiency to highlight its importance in the current world's cyber safeguard.

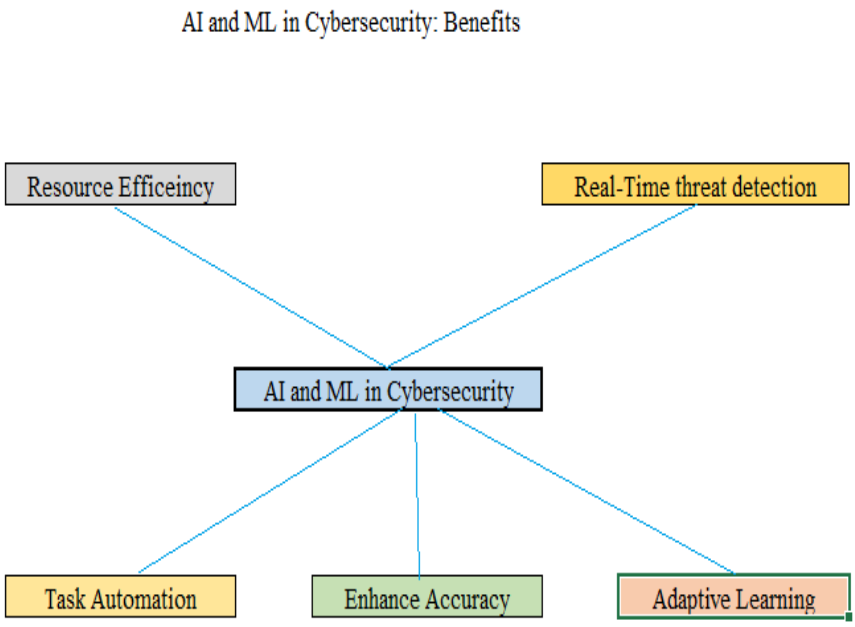
8. APPLICATION

Integrating Artificial Intelligence and Machine Learning into cybersecurity delivers immense value and alters the way that organizations identify, avoid, and mitigate cyber threats [1]. The first benefit is threat identification in a real-time sense; large data sets are scoured by the AI and ML for threats beyond the capacity of analysts. Al this leads to faster response rates and also cuts on the amount of risk sustained by the affected company.

The same way AI learns from the pattern that exist in the data it also makes it accurate in terms of identifying new types of threats that are potential such as the zero-day vulnerability and the advanced persistent threats. Furthermore, and primarily, machine learning allows for constant improvement through the use of such concepts as adaptive learning in which models can improve or modify themselves and their approach through new data and patterns of attack.

AI also executes process-oriented tasks, as logs analysis and incident prioritization, and emancipates cybersecurity experts from mundane work. Also, AI-Integrated systems utilize resources most effectively since the alerts concerning threats are presented under different priorities so that critical threats are the most urgent. Lastly, AI and ML greatly enhance cybersecurity by offering solutions to increasingly complex threats at a considerably faster, more accurate, and on a large scale.

Currently, AI and ML are transforming cybersecurity from an almost entirely traditional prevention measure to a proactive approach to defence. When it comes to appreciation of these technologies in relation to their development these technologies are expected to evolve even further so as to get rid of these ever-changing threats in the cyber space. Key developments include:



8.1. Autonomous Cyber Défense

Stand Alone Self-Acting describes systems based on AI which work independently to identify, control and dismantle Cyber-Security Threats without human inputs. These systems employ the use of machine learning algorithms to study the patterns of flow of traffic in a network, the resulting logs from applications and the behaviors of users to detect signs of threats. Different from them is the fact that they are capable of making changes to their strategies of attack in the light of previous lessons. For example, when a new type of the virus exceeds the protection, the system modifies its diagnostic programs in order not to allow such cases again. The autonomous defense is most useful in extensive networks for the reason that there is simply too much data being processed to allow for personal monitoring. These systems are designed to work in reverse or real time and help quarantine affected devices, kill the offending process, and prevent the leak of the hole across the network, which greatly improves an organization's security.

8.2. Countering Quantum Computing Risks

That is why with emergence as a new technology of quantum computing, it poses great threats to traditional cryptographic solution. This is where quantum computing will help to develop quantum immune algorithms while using AI and Machine learning to show the vulnerabilities in current encryption models. Same technologies shall also assist in hindering the attacks that will be made possible by quantum capabilities, ensuring security and reliability of data in the new quantum world. Therefore, further development of capabilities in the context of using AI and ML in cybersecurity will follow the relevance of the adaptability of AI-based systems and integration of cooperative learning technology, optimizing interfaces between human and machines, and readiness in using quantum technologies in attacks; this prepares a highly progressive agenda for PACS.

8.3. Self-guided Cyber Security

On the basis of AI, Stand Alone Self-Acting defines systems that implement a sole mode of operation to detect, monitor, and neutralize Cyber-Security Threats without human intervention. These systems utilize the technique of machine learning to analyze flow of traffic within the network; logs from applications; and the behavior to look for signs of threat. Unlike them they can mutate their strategies of attack in the light of lessons learnt from previous encounters. For instance, when a new type of virus goes beyond the protection, the system adjusts the diagnostic programs to ensure that it is impossible to record such incidences. And finally, the autonomous defense is most useful in extensive networks for the reason that, well, there is simply too much data being processed, that personal monitoring cannot possibly occur. These systems should work inactive or in real mode and assist in isolating compromised systems, terminating the suspicious process, and stopping the leakage of the hole across the network, which enhances an organization's security significantly.

8.4. Federated Learning

Federated learning is an innovative approach where awesome AI models are trained over decentralized data, say, several organizations or several devices without getting into the particulars with raw data. In cybersecurity this approach promotes partnership between organizations in the improvement of threat detection and response as well as privacy and data protection and compliance with General Data Protection Regulation. For example, the federated learning system is in a position to identify the attack pattern that has been noticed in different companies while it is not forwarding its internal data. This also suggests that there is a better and more encompassing logic for coordinating the act of protecting cyberspace that Favors all actors. In the same regard, federated learning also preserves the data security at the time of training by employing the encryption and secure multiparty computation technologies that make it the strong and innovative technological platform for the collective defense against cyber threats that are challenges of the contemporary global society. Artificial Intelligence in Formal Decision Systems Rom a purely reactive practice to a strategic and predictive defense strategy. As advancements in the field of technology are regarded, these technologies are poised for further evolution so as to do away with the constantly evolving threats in the cyber world. Key developments include:

8.5. Interpolating AI into Formal Decision Making

The latter is applicable in enhancing the general capacity of human managed cybersecurity teams by providing new syntactic and/or semantic perspectives and/or recommendations. In cyber events, [SIH] treats threat information, network occurrences, and system opportunities in pursuit of the finest response strategy. For example, if the ransomware attack is identified then an AI system may recommend that servers must be shut down, some specific IP address should be blocked, and backups must be utilized. The selection strategies are very fast especially when human operators are provided with several response choices with other subsequent events expected by the AI. These tools are very useful in some ways, especially when used to reduce the volume of load to the analyst who deals with a large number of alerts. Last, the access of the artificial intelligence as well as integration of artificial intelligence in decision making assist in eliminating the hypes between automation and work from incidence handling.

8.6. By The Use of Countermeasures

Arguably one of the main issues that quantum computing is going to condemn about present day cryptographic practices is with regards to attacks from algorithms like Shor's. Of such risks, AI is

anticipated to play the leading role in addressing them. Firstly, AI can assist in developing new one's post-quantum cryptographic algorithms for communication security as well as the safeguard of information in the future [8]. Second, AI systems are capable of the analysis of threats related to quantum technologies and also can simulate respective attacks on existing infrastructures. For instance, AI can recommend systems that are most susceptible to quantum decryption, and which may require change in their encryption paradigms. Besides, it also reveals opportunities for organizations changing the current protocols, which could make them quantum-safe when using new technologies as it would be easier to automate the alteration too. This approach will safeguard the information from its future threat that quantum computing will pose.

9. DISCUSSION

On the same note, [4] and [2] pointed out that Artificial Intelligence (AI) and Machine Learning (ML) are revolutionary features in cybersecurity.

[4] in their paper, The AI Revolution in Cybersecurity identified that behavioral analysis tools as a result of artificial intelligence are critical for dealing with insider threats and accounts that have become compromised. They state that due to these attributes, it can create behavioral profiling and detect deviations that suggest an attack is under way. This research further augments their works by showing real-world examples like a financial institution that uses AI to recognize abnormal login timings and unauthorized file downloads where AI could play the part of stopping security breaches triggered by insiders.

[2], in their work "Intrusion Detection Systems with Machine Learning: "A Comprehensive Survey," in order to understand how ML refines the recognition of known and novel risks. They illustrate the major disadvantages of IDS, based on the static approach and pattern matching that have been described above and show how approaches based on supervised learning (for example, Random Forest) and unsupervised one, such as K-Means clustering can help detect anomalies and even zero-day threats. This research enhances their work by providing a real-world implementation of the framework and the application of ML for DDoS attack and traffic anomaly-based insider threat identification.

10.Conclusion

Several AI techniques are applied to cybersecurity as they allow for real-time threat detection and response, dynamic approach to threat intervention, and intervention based on new patterns in cyberspace. These technologies improve intrusion detection solutions, behavior profiling, threat intelligence and ransomware protection with preventative tools that help mitigate exposure and reaction time. Indeed, incorporating human-centered solutions with artificial intelligence tools makes frameworks much more effective in cybersecurity. Nonetheless, adversarial attacks, and data biases show that the problem requires proper defense and ethical application. In total, AI and ML are the critical components for constructing secure digital environments and developing new approaches to fighting complex threats and protecting today's information assets.

REFERENCES

[1] A. ALSHAIKH, M. Alanesi, D. Yang, and A. Alshaikh, "Advanced techniques for cyber threat intelligence-based APT detection and mitigation in cloud environments," in International Conference on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2023), P. Loskot and S. Niu, Eds., SPIE, Jun. 2023, p. 65. doi: 10.1117/12.2681627.

[2] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K. Il Kim, "Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection," Electronics (Switzerland), vol. 11, no. 23, Dec. 2022, doi: 10.3390/electronics11233934.

[3] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Mar. 01, 2023, MDPI. doi: 10.3390/electronics12061333.

[4] N. Kaloudi and L. I. Jingyue, "The AI-based cyber threat landscape: A survey," Jan. 31, 2020, Association for Computing Machinery. doi: 10.1145/3372823.

[5] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, "Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review," International Journal of Software Engineering & Applications, vol. 13, no. 5, pp. 13–21, Sep. 2022, doi: 10.5121/ijsea.2022.13502.

[6] U. A. Butt et al., "A review of machine learning algorithms for cloud computing security," Sep. 01, 2020, MDPI AG. doi: 10.3390/electronics9091379.

[7] A. Al Mamun, H. Al-Sahaf, I. Welch, and S. Camtepe, "Advanced Persistent Threat Detection: A Particle Swarm Optimization Approach," in 2022 32nd International Telecommunication Networks and Applications Conference, ITNAC 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 42–49. doi: 10.1109/ITNAC55475.2022.9998358.

[8] P. Radanliev, "Artificial intelligence and quantum cryptography," Dec. 01, 2024, Springer Science and Business Media Deutschland GmbH. doi: 10.1186/s40543-024-00416-6.