Improving Cybersecurity Systems Using Artificial Intelligence Techniques

Ismail A. Humied[1]

[1]*Associate Professor, Faculty of Police, Policy Academic, Ministry of Interior, Sana'a, Yemen*
dr.ismail_humied@yahoo.com

Abstract

Cyberattacks and threats are in complexity every day. With the number of attacks growing every day around the world, there are a variety of methods and strategies for penetrating business systems and individual devices. Individual attackers, organizations, and whole nations are responsible for these attacks. Attack resources are growing and cyberattacks can have severe global impact and consequences. These variables make it difficult for security teams to keep pace, so smarter solutions are needed. This research provides an overview of how two areas of artificial intelligence (AI), machine learning and deep learning, can be used to meet cybersecurity challenges. The research can also show how existing AI technologies can improve cybersecurity. Security systems can use AI to automate time-consuming manual security operations and make detection and response more proactive and predictive. As part of this research, a workshop was held with official from government and private agencies, who are responsible for network monitoring and security. During this workshop, a discussion occurred what problems individuals had at work. Thus, this research includes potential AI-based remedies for identifying issues.

Keywords: *Artificial Intelligence, Machine Learning, Deep Learning, Cybersecurity, Cyber-attacks, Cybercrime, Detect.*

1 Introduction

Computers are indispensable in today's workplace and daily life. The development and spread of modern technology have increased the need for information security. The amount of data collected is enormous and is constantly being driven by commercial, military, financial, medical, and government applications. This highlights the importance of cyber security. The term "cybersecurity" is widely used and is an issue that we must constantly address and move forward. Cybersecurity is the process of protecting data and information on networks, mobile devices, computers, and other electronic devices

or connections. It is sometimes called computer security or information technology security. In addition to preventing harmful attacks, unauthorized access, and other harm, the objectives are to guarantee the data's integrity, availability, and confidentiality [1, 2].

Most of our computer systems and network infrastructure are connected via the Internet. Virtually all businesses, governments, and even individuals today rely on cybersecurity to protect their data, grow their businesses, and protect their personal information. People send and receive data over the network infrastructure. Routers are vulnerable to external hacking and tampering. Big data has emerged as a result of increased data volume and complexity due to increased internet usage. Due to the constant growth of the Internet and the amount of data it contains, it has become necessary to develop a reliable intrusion detection system. The network security subset of cybersecurity protects networked systems from unwanted activity. Networked computers become available to ensure data confidentiality, integrity, and accessibility. Current cybersecurity research focuses on developing reliable intrusion detection systems that can detect both known and new attacks and threats with high accuracy and minimal false alarm rates [3].

The most commonly used rule-based systems today are used to implement cybersecurity. The method used to teach a system rule to understand how to process, store, and sort data is called a rule-based system. The system manufacturer or vendor implements the rules. Rules can often be changed by updates. In the event of an attack, the system searches through a set of rules to find the correct answer. If no action is taken to counter a particular attack, the system should be shut down. The designer then has to detect the problem and manually fix the system with a patch or software upgrade [4, 5].

Rule-based systems are not amenable to modification and customization, resulting in a very high rate of new attacks and variants of the same attack. The tedious remediation process of these stubborn attacks takes a lot of time and effort, reducing production and efficiency. Addressing these issues requires designing systems that can adapt to their environment, learn from experience, and change rules to counter future adversarial attempts. This means that the system can patch itself and figure out how to fix vulnerabilities on its own. Additionally, the system can track past attacks and rebuild the system based on newly created rules [6].

To solve the above problems, cybersecurity can use artificial intelligence (AI). Cybersecurity products based on artificial intelligence have become more popular and have evolved rapidly over the past decade. The expansion of these technologies will improve the effectiveness of cybersecurity-related tasks and reduce the frequency and risk of security breaches [7, 8].

The purpose of this research is to show how cybersecurity can be advanced by systems and techniques based on artificial intelligence. There are many facets to AI, and this study does not explore them all. Moreover, there are so many types of attacks that it's impossible to cover them all here. The main purpose is to see real systems already

in place and how they can be used for network security. Intrusion detection systems are getting better at detection and remediating anomalous activities and potential threats as more AI techniques are integrated into computer security. Finally, the study seeks to shed light on the obstacles hindering the continued growth of the use of AI tools in cybersecurity and the prospects for AI in this area.

This research starts by descript machine learning techniques and deep learning techniques. In the next section, the presents analysis, possible solutions and current techniques from the workshop conducted and the individual meetings of participants after that are presented. Finally presents the discussion and conclusion.

2 Methodology

Literature research and workshop results were used as research methods in this research. A general literature review was conducted to learn more about the field of AI and cybersecurity. The literature survey first aims to provide an overview of artificial intelligence and various cybersecurity practices. Then, in the background, we discuss the theory of machine learning and deep learning; and how these techniques can be used to detect intruders and attacks. On November 3, 2020, in the meeting room of the Ministry of Communications and Information Technology, a workshop was held with the participation of thirteen responsible and specialists from several government and private agencies, which its results were used as a second technique in this research. During this workshop and the individual meetings of the participants after that, a discussion occurred to detecting concerns about network security and monitoring; and suggestions for improvement. Thus, this research includes potential AI-based remedies for identifying issues.

This study used qualitative research as a methodology. The focus is on individual and group actions and perspectives. Subjective opinions and observations often form the basis of qualitative research, there may not be many participants at the workshop, but a lot of information flows and enough data are collected to answer the questions. It is important that participants are suitable for the study and are carefully selected [9].

In qualitative research, a deductive technique involves a thoughtful, predefined rationales with clear connections between research and meetings. Thematic content analysis and narrative analysis are her two subsets of the inductive technique. looking for recurring themes and patterns in the material collected from participants. Participant comments are analyzed and the most important findings are highlighted [10]. A thematic content analysis technique was chosen for this study.

The first part of the workshop focused on the current network and security monitoring tasks and the types of activities each participant performs on a regular basis. Participants were then asked about the types of problems they encountered in performing their duties and how those problems affected the monitoring and security elements. Suggestions for improvement were also considered. I wrote down the problems and suggestions for improvement, then typed it up. It is difficult to have a general dis-

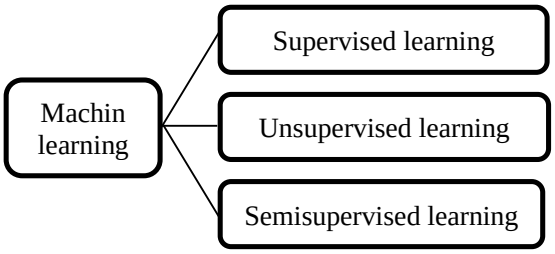

Figure 1: a taxonomy diagram of the machine learning algorithms [8]

cussion about AI due to the lack of specific AI expertise among most of participants. In hindsight, this was not ideal, as a more complete explanation of AI technology and how to use it would have been very helpful. I had no access to or training in network monitoring tools, this was another limitation for the study.

3 Machine learning techniques

The question whether a general-purpose computer should look at data and generate rules rather than relying on humans to generate them was raised by Alan Turing's assertion that computers can learn and determine their uniqueness. Techniques that can learn from data and adapt are called machine learning techniques. Machine learning techniques are created to generate results based on what is learned from the data and examples. For example, such techniques will allow a computer to select and perform certain innovative traffic detection tasks without explicit instructions [11].

Machine learning can be effectively used to perform automated evaluation of attacks and security events such as spam emails, user identification, social media analysis, and attack detection [3]. Supervised, unsupervised, semi-supervised, and reinforcement learning are the three primary methods used in machine learning. Supervised learning is based on labeled data, unsupervised learning is based on unlabelled data, and semisupervised learning is based on both [12], as shown in Figure 1.

4 Deep learning techniques

The main difference between these two methods is feature selection. Unlike ML, where selection must be done manually, feature selection in DL is automated. The goal of DL techniques is to better understand the input data and extract data qualities that are difficult for humans to perceive [13]. Machine learning methodologies are also utilized in deep learning. owever, other ways are employed in deep learning, such as Transfer Learning [8], as shown in Figure 2.

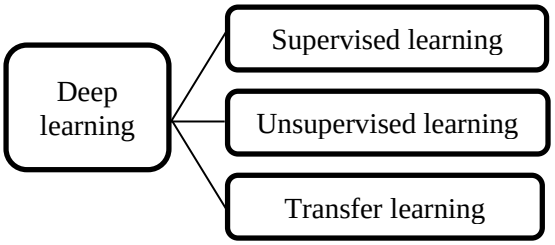

Figure 2: a taxonomy diagram of the deep learning algorithms [8]

5 Analysis, solutions and current techniques

This section presents analysis of workshop discussions, and possible solutions and current techniques which we can used.

5.1 Analysis of workshop discussions

In this subsection, a description of the discussion and notes taken during the workshop and the individual meetings of participants after that.

Director of Information Security - Yemen Mobile Company: this participant claimed that lack of visibility of network data was the biggest problem with network monitoring. Although no specific solutions were presented in this workshop, participants were intrigued by the potential application of AI to detect anomalies. We also explored what changes and adjustments should be made to existing networks to facilitate automation of anomaly detection anomalies.

Director of Information Systems and his two employees - Ministry of Communications and Information Technology: also, these respondents raised the concern of data visibility. Latitudinal mobility and methods for spotting potential assaults and threats inside the network were the specific types of network visibility that were covered. After they have gained access to the network, attackers exploit lateral movement to penetrate farther. One respondent mentioned a number of technologies, including security operations, automation and response technology, and Network Detection and response systems. According to the three respondents, these kinds of technologies were important for the ministry 's upcoming network security and monitoring goals. Moreover, skill certification was listed as a potential upgrade for the future.

Assistant Undersecretary for Technical Affairs at the Ministry of Communications and Information Technology: the topic of data visibility was also brought up by this participant. He claimed that the technology used does not provide real-time insight and alerts on network anomalies and risks. Endpoint detection technology and the potential to improve the monitoring process were mentioned by the respondent. Interesting topic he is one. He said researching techniques to increase the visibility of lateral movement and the hazards it poses will be another important feature in the future. Members of the Teaching Staff - Higher Military Academy: the issue of network visibility was also

raised by the participants. Respondents said that additional monitoring and carefully selected tools designed for the specific problem would be the answer. The idea behind the recommended technique was to streamline surveillance activities and increase their effectiveness.

Director of Information Security - General Post Authority: a key point for the participant in this conversation, also related to data visibility. According to the person, data about anomalies under investigation may lack relevant information, so one remedy is to learn more about the causes and underlying problems of anomalies. Custom development is another key component of network monitoring that the participant pointed out. According to the participant, this makes it easier to match the infrastructure with the authority's needs.

Director of Monitoring and Control - Public Telecommunications Corporation: this participant raised the possibility of improved alarm handling and alarm accuracy. Participants hope that in the future, incident managers will take a more active role in building and improving surveillance systems, resulting in more reliable system output and more accurate warnings. This participant suggested intelligent monitoring and creating easy-to-understand dashboards that monitoring teams could use as tools.

Director of the College of Postgraduate Studies - Police Academy and director of the Command and Staff College - Higher Military Academy: These two participants emphasized the management aspect. They noted the importance of clearly assigning and delegating responsibilities for various aspects of the monitoring and security process. In-house skills were also a factor, they said, and felt that this strategy should be promoted in the future. It was determined that some planned software improvements would require major hardware refreshes, which is neither feasible nor beneficial from a cost-effectiveness standpoint. Another technical issue was the difficulty or impossibility of linking the colleges' specific software to other system security colleges.

Director General of Cisco Academy - General Institute of Communications: this participant pointed out that some monitoring tasks and root cause analysis are still done manually. According to this participant, more automated techniques for detection of anomalies would be the solution to this problem. Participants specifically recommended that automatic feature selection can reduce some human effort. Participants also expressed a desire for staff to receive additional training on surveillance-related responsibilities in the future. According to the participant, one of the possible remedies, he said is skill certification, which will enhance the overall oversight process.

Director of Information Systems - TeleYemen Company: according to this participant, the existing system is too passive. This individual was interested in how AI could increase the aggressiveness of network monitoring systems and how AI-based systems could provide more real-time data and information. Attendees were also interested in AI-based products on the market and how they can be used to help companies.

Information Systems Consultant - General Post Authority: this participant found that some devices connected to the internal network did not have enough information during their daily work. Future solutions this participant hopes will include richer

endpoint data and more real-time network traffic statistics. Participants made these suggestions to increase the effectiveness of their Workshop outcomes.

The first four participants brought up the visibility of network data. The data relevance and relevance of pertinent information about network traffic and networked devices are closely tied to the visibility issue. Directors of Information Systems bring up these kinds of problems. The collecting and analysis of data traveling inside the network as well as into and out of the network constitutes visibility in terms of network monitoring. East-west traffic is a term used to describe traffic that travels from one server to another inside a network.

Director of Information Systems and his two employees and Assistant Undersecretary for Technical Affairs at the Ministry of Communications and Information Technology raised concerns about lateral or east-west traffic monitoring. Around half of the participants brought up visibility-related issues. The fact that participants from other teams or agencies also mentioned this issue demonstrates the broad impact the visibility issue has. This makes it quite evident that in order to address this in the future, suitable solutions and action must be taken. An organizational network's visibility is essential in many ways. Visibility of network data is essential in a setting where the frequency of cyberattacks is rising.

Real-time network data and information were the second most common issue of the workshop. Real-time data is crucial because it enables monitoring and security teams to respond to threats and anomalies more quickly. Director of Information Security - General Post Authority and Assistant Undersecretary for Technical Affairs at the Ministry of Communications and Information Technology raised this issue. This problem is especially worth detection and recognizing because they have diverse job descriptions and duties.

Other top priorities are problems with alert processing and alert accuracy. The importance of alert accuracy makes issues with it a typical occurrence in network monitoring. More automated detection techniques have a byproduct of false positives and false negatives. This topic was only mentioned by one person (Director of Monitoring and Control - Public Telecommunications Corporation). Yet, this does not imply that the problem is unimportant, and the accuracy of the alerts is a crucial component of any security monitoring system. User and Entity Behavior (UEBA) can offer solutions to improve alert, confidence, and accuracy.

The monitoring procedure, including feature selection, still involves several manual chores, according to Director General of Cisco Academy. The application and use of DL to this problem is possible.

A few more themes that cannot be resolved by AI were also raised by the attendees. Finding solutions that are carried out internally was a prevalent subject that came up in the workshop. This gives the business more control over the design and system infrastructure. Regarding monitoring, this helps the agency to find solutions to issues more quickly without having to wait for input from providers. Director of the College of Postgraduate Studies - Police Academy and director of the Command and

Staff College - Higher Military Academy discussed the administration of the system. Clear management and well-defined goals are necessary for the continued growth of the monitoring and security system in order to enhance the system.

5.2 Solutions and current techniques

As a part of my task at the workshop, I had to find and present AI-based solutions and techniques. The purpose of this section is to propose solutions and current techniques to the problems brought up by the participants. This section describes the design principles needed to create an ML-based recognition system and the factors that need to be considered. One of the main themes of the workshop was how to move from reactive to proactive action, so planning for systems should be emphasized. Moreover, the role of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in network security and monitoring is discussed. Some typical surveillance systems use AI. IPS and IDS concepts and technologies are moving towards so-called Network Detection and Response NDR systems. Therefore, in the next subsections, we will discuss how to develop detection, response systems and AI-based strategies to address many of the issues raised at the talks. Together with AI-enhanced security operations, this section also discusses unsupervised learning techniques.

5.2.1 Machine Learning Anomaly Detection Systems

Today, any agency must regularly analyze its network data for trends. A large part of network monitoring is finding anomalies. A data analysis process called anomaly detection looks for unusual and irregular patterns in data. Deviations from standard network behavior and their identification are essential so that network administrators can take action and respond to attacks and hacking attempts. AI can be used in this process. Anomalies can be classified in different ways, depending on the type of anomaly and the context in which it is examined. A particular data point or instance that appears to deviate from the typical metric value of the dataset is called a point anomaly. Contextual anomalies are anomalies caused by the specific context and facts of a situation. For example, some periods or seasons are expected to deviate from typical data behavior. However, if this occurs outside the expected time frame, it is considered an anomaly of context. Groups of data instances that collectively deviate from normal network behavior are collectively referred to as collective anomalies. A single anomalous result is not considered an anomaly in this scenario [14].

Manual techniques are still commonly used to detect anomalies. A weekly reviewed dashboard is a popular way to monitor a network. Personnel monitoring the network watch for spikes and dips in traffic, her activities and see if they are abnormal. This method is limited to the original collection of measurements and is difficult to scale. This method can detect large anomalies, but may not easily detect small anomalies. Many attacks today are more scattered and short-lived, so the system may not even know what to look for. Reviewing the dashboard after an anomaly has already occurred

significantly slows the incident response time. Manually setting thresholds on selected metrics is another way to detect anomalies. This technique relies on alerts being sent when metric measurements deviate from thresholds. Setting the thresholds correctly is essential for this strategy to work, but it can be difficult even for small networks as there are hundreds of measurements and functions to consider. Setting the threshold too high or too low will increase the number of false positives. Anomalies can also go unnoticed if the limit constraints are not specified correctly [15].

Several participants pointed out problems with real-time information and expressed a desire to further automate the anomaly detection process in the future. There are five key design elements that must be considered throughout the planning phase of an ML-based automated anomaly detection system [15]: Event timeliness, scale, rate of change, conciseness, and definition of incident.

The Event timeliness deals with the question of how quickly anomalies must be discovered. Alerts for attacks, threats, and identified dangerous network activity are part of real-time anomaly identifying. Enterprises should be aware of this factor as it influences the choice of which type of ML technique to apply and the tasks and goals for which it is used.

The infrastructure and execution of detection systems are highly dependent on scale and data amount. Different monitoring activities use different record sizes. In this case, it is important to examine whether the system works with large amounts of data or small amounts of information. ML and DL techniques react differently to data volume and labeling, or lack thereof, so the planning of the system is affected.

Rate of change is the rate of change of the measured data. Change rate affects the ML or DL technique used for a task, depending on the metric being monitored. Systems may experience frequent changes in measurements during network monitoring, so to work effectively, techniques must include adaptive properties.

Conciseness is the idea that a large number of measurements and factors should be considered when detection anomalies. This concept helps provide users and systems with a comprehensive view of the root cause of anomalies. Often, looking at just one measure doesn't tell the whole picture. For example, a system upgrade in one region may cause delays in another region. The conciseness of ML anomaly detection system can be a technique in three different ways. Each system metric is used by Univariate Anomaly Detection to create a map of typical behavior.

This technique scales easily because each instance is handled independently. Root cause analysis is not possible with this technique, and many anomalies are generated by one unexpected event affecting multiple metrics simultaneously. Multivariate anomaly detection takes multiple inputs and analyzes them together. We combine these metrics to create a virtual event model. This has the disadvantage that the anomaly output does not indicate the parameter that caused the anomaly. In order for the system to have the required computing power, the input signal types must be identical. The hybrid technique of these two methods takes a univariate single metric technique, but explores the relationships between anomalies rather than grouping many of them in a black box.

This gives better results when conducting root cause analysis.

Definition of incident is the final design principle to consider. A fully automated system for detection of intruders and anomalies is not yet feasible, so it remains necessary to determine what defines an event. A complete description of the event requires detection of all, or at least most, causes of the anomaly. This works for systems with a limited set of parameters and metrics, which is usually not the case. At this stage of system design, the ML and DL concepts of supervised, unsupervised, and semisupervised learning should be considered. Supervised methods are appropriate when some measures are clearly specified and the goal of the system is to provide classification or regression. For these techniques, to establish a baseline of typical behavior, the training data needs to be tagged. This technique is not very effective at detection new intruders or anomalies due to supervised learning-based anomaly detection training models.

Unsupervised learning is a valid strategy in most cases because it can be difficult to predict all possible situations. An unsupervised procedure identifies anomalies whenever the investigated data deviates from the trained model, and the system gradually learns typical system behavior. The training dataset is unlabeled, so the system can detect new incidents, whether known or unknown. The success of unsupervised learning depends on how accurately and completely the behavior of a typical system is described. This makes the training phase essential as it sets the thresholds and the framework within which the technique operates. Combining these two techniques creates a better methodology.

This is achieved through semisupervised learning. Here, the technique trains on a sparse set of labeled data to understand the input structure. Combining supervised and unsupervised techniques often gives the best results for anomaly and intruder identifying. Intrusion and anomaly automation fundamentally relies on the notion of normal or abnormal behavior. Any approach for detecting anomalies generally works by gathering data, determining what is normal, and then using a statistical test to determine if any subsequent data point in the same time series is normal or abnormal. Such as the shaded region in Figure 3. Below was created as a result of such statistical analysis. So, we might use statistical tests to identify any data point outside of the shaded region as abnormal and any data point of it as normal.

The input data for the network is often very large, but it can also be unpredictable and nonlinear. Combining several different models is a more reliable option to create a correct baseline, as it is impossible to simulate typical behavior. Seasonality is an important factor to consider when creating baselines, and failure to do so can result in contextual anomalies. Second, because ML and DL techniques periodically update new normal values based on incoming data, anomalous data points are subject to the fact that they change the baseline and to prevent or produce erroneous results in the future, it should be given less weight [16].

Output rendering in anomaly and intrusion detection is often problematic. The significance of an anomaly should be expressed in some way when designing an detection system to determine how far an anomaly deviates from the normal and how the system should respond. Scoring and binary metrics can usually be used to label anomalies.

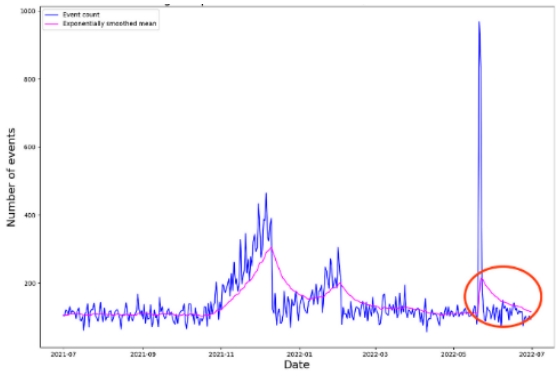

Figure 3: The data points outside of the shaded region are anomaly [15]

Score-based detection assigns a score to the amount by which an identified anomaly deviates from a specified normal norm. Anomalies are ranked according to their scores and can be further investigated. The second method, binary classifies instances as either normal or abnormal [14]. In other words, the system should be able to assess the relevance of anomalies to intruders and react only when necessary. The result is fewer pointless alerts and less manual work for network analysts.

Understanding how metrics are related and how they could stem from the same root cause is a challenge related to the problem of many alarms being active at the same time. Therefore, learning behavioral topology is of great importance in the development of automated systems. Investigating the occurrence of anomalies and determining whether there is a causal relationship between them is one way to detect commonalities in anomalies. The use of clustering techniques is a machine learning technique for determining causality [17]. Clusters can then be represented using the two techniques described earlier (scoring and binary labeling). The Latent Dirichlet Assignment (LDA) technique is a popular candidate for clustering big data. To find the underlying patterns in the data and understand how different sections of the data are related, thematic modeling uses his LDA, a machine learning technique [18]. Often data points are classified as belonging to only one class using clustering techniques. LDA has the advantage that measurements can belong to more than one class and commonalities can be found between them [17]. A strategy for intruder detection using the LDA technique was proposed by Huang et al. [18].

5.3 Intrusion Detection System

Intrusion detection systems (IDS) are one of the best known areas of cybersecurity using ML techniques. This section describes how IDS works and how to create an IDS taxonomy. IDS is a security software that automatically notifies network administrators when hostile activity, system compromises, and security policy violations occur [19]. IDS uses hardware solutions or software embedded in firewalls to monitor networks and

detect malicious network traffic. Security information and event management systems often combine the output of network resources into hostile activity reports, Security information, and event management (SIEMs). An IDS is one part of a system that includes firewalls and intrusion prevention systems (IPS). However, there are significant differences in the functionality of these components. IPS is similar to IDS, except that the system has the ability to disconnect the network. An IPS is an active, inline threat protection system, often placed right behind a firewall. In contrast to IPS, IDS is a passive system that observes network packets and identifies potentially malicious behavior by comparing signature patterns to predefined typical patterns [20, 21].

There are two types of intrusion detection systems [20, 19]. Both host-based intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) monitor operating system files and network traffic, respectively. NIDS works by distributing sensors throughout the network to monitor network activity. HIDS is a host or device-specific implementation and only tracks traffic on that host or device. Both NIDS and HIDS use two techniques to detect malicious network traffic: signature-based attack detection and Anomaly-based attack identifying.

The basis of signature-based intrusion detection is the identification of identified threats. This technique requires a predefined set of indicators of compromise to scan the traffic for. Byte sequences, file hashes, and email subjects are examples of indicators. When the system identifies a suspicious network activity, it observes the packet, compares it to a database of threat indicators, and flags the packet [22].

The second technique, known as anomaly-based intrusion identifying, uses machine learning techniques. Here, the system uses ML techniques to train the detection engine to detect typical behaviors and create a baseline. This strategy compares network behavior to the norm rather than looking for threats. This means that the system will sound an alarm if the behavior deviates from the norm. This method has advantages over signature-based strategies in that it can detect unknown threats [22]. The majority of surveillance infrastructure and systems use IDS and IPS. Nonetheless, there are some issues that hinder some components of the monitoring task. The primary purpose of IDS is to track north-south network traffic. Client/server traffic entering or exiting a network or data center is referred to as north-south traffic. In other words, IDS can detect risks and anomalies originating from networks outside the organization network. IDS cannot detect attacks inside the network [23].

Lack of visibility into internal network traffic such as Server-to-server or called east-west transmissions are problematic. Moreover, the IDS technique relies on a signing library, so it cannot detect new attack types. Moreover, automated analysis and investigations require human involvement or cooperation with IPS [23]. Like IDS products, intrusion prevention systems have some disadvantages. A large data set generates many meaningless alarms and IPS cannot separate the relevant signal from the noise. To effectively detect threats and anomalies, IPS solutions use signature models that need to be updated frequently [24].

While IDS and IPS technologies are essential components of any security operation

and cannot be replaced, there are techniques that can address the above issues. Gartner's security operations center visibility triad represents a new development in network security. In the next section, we'll take a look at it.

5.4 Gartner's security operations center Visibility Triad

The SOC Visibility Triad was first mentioned by Augusto Barros, Anton Chuvakin, and Anna Belak in their March 18, 2019 Gartner research paper titled "Applying Network-Centric Approaches for Threat Detection and Response." The rising sophistication of threats necessitates companies to leverage many sources of data for threat detection and response, Gartner says in this note. Composed of three components called SIEM, EDR, and NDR, this idea enhances visibility of network traffic, reduces attack response time, and helps to detect various types of East-West attacks [25, 26].

5.4.1 Security information and event management

A software program called Security Information and Event Management (SIEM) is used to log and collect network data. SIEM brings this data gathered from applications, endpoints, cloud services, and security devices, and collects them in an integrated manner. Threats and events can be classified based on this aggregated data and alerts can be generated based on defined criteria. AI-based UEBA technology is incorporated into SIEM methodology. The process of creating network baselines is more automated using UEBA [27].

5.4.2 Endpoint detection and response

The second component of the visibility triad is endpoint detection and response (EDR) technology. The role of this technology is to detect malicious data and traffic on endpoints such as servers and laptops. EDR uses behavioral analysis on top of traditional antivirus software to detect risky activity [27]. EDR is a complementary technology to SIEM, and the two parts have long served as the foundation of security operations. An endpoint system can detect this behavior and flag it as an anomaly, but the log could be corrupted by an attacker, resulting in the threat not being reported by her SIEM [27]. Security operations personnel can use EDR technology to isolate infected endpoints from the network and prevent lateral spread of threats.

5.4.3 Network Detection & Response systems

The Network Detection and Response systems (NDR) represent a new development in network security and it is the latest addition to the Triad. NDR technology complements here, EDR, and SIEM methods by enabling detection without the use of rules or signatures that govern system operation [28]. By using carefully placed sensors, NDR can monitor east-west communications in addition to monitoring north-south traffic at the network perimeter. Advanced NDR systems can detect novel unknown attacks. The

NDR system uses AI technology to provide businesses with enhanced detection capabilities. Furthermore, ML has given the NDR system the ability to more accurately assess threat levels [29]. It is important to emphasize the complementary nature of triads. Endpoint detection systems require continuous monitoring and maintenance, reducing internal network visibility. NDR uses behavioral analytics supported by ML and AI-based techniques to detect threats propagating and communicating between intranet devices. A more reliable security architecture is created by NDR's real-time monitoring capabilities and EDR's signature-based technology. Additionally, the NRD system uses a cloud-based ML technique to reduce tedious modeling work and reduce system load. In addition, NDR introduces the ability to automatically update its signature database and detection models using machine learning techniques. Real-time network information provided by the NDR component can improve the EDR system's ability to isolate specific endpoints from the network [25].

SIEM systems are a popular method used by companies for security operations because they are effective at recording data. With well-defined parameters for malicious behavior, SIEMs are typically able to detect threats early. Data analysis by SIEM systems leads to a large number of false alarms. This is an undesirable result when using security systems. Due to the large amount of data generated in large organizations, network traffic logging is disabled at certain times of the day or week. As a result, there is a window for attackers to launch attacks and delete or modify previous logs, making attacks difficult to detect. Wire data (network packets) is used in the NDR system to show network communication and paths through the network. Wire data, unlike log data, is immutable, providing SIEM systems with complete and reliable metadata to perform their functions [25].

5.5 Unsupervised learning techniques

In this subsection, we shall present three patented unsupervised learning security techniques.

5.5.1 Enterprise Immune System

The system uses unsupervised learning techniques to detect and block known and unconfirmed malicious network traffic. This method addresses the problem of rule-based systems by learning from data to create models of both normal and deviant behavior [30]. An example shows how the AI component of Darktrace's company solution can detect ransomware attacks in real time and react to them [31]. In one case, an employee accessed a malicious word document via a work email, allowing ransomware to enter the network. The employee's computer started connecting to suspicious external sites and searching for SMB shares. SMB or Server Message Block is a network protocol that allows files to be shared between devices connected to the same network [32]. Additionally, the ransomware can start encrypting SMB shares and have a detrimental effect on the entire corporate network. There were no employees on site as the incident occurred

after business hours. The enterprise immune system detected this within 9 seconds, and after 24 seconds the engine stopped cryptographic operations, fixing the problem without human intervention. Due to the fast response time of the system, only a small portion of the network was slightly damaged. Detection of these threats is easier using unsupervised learning techniques, as demonstrated by the Darktrace case.

5.5.2 Vectra Cognito

Vectra AI company develops an NDR cybersecurity platform with AI-driven attack behavior detection [33]. Vectra Cognito is the name of the proposed system, and it claims that, similar to the enterprise immune system, Vectra AI can learn the system's behavior and capabilities in detecting threats. Instead of using all available network data, Vectra Cognito collects useful enriched metadata to give you a clearer picture of your system. This feature also reduces noise in the data using SIEM and EDR systems.

5.5.3 Security operations, automation, and response technology

A relatively new tool and implementation idea in network and cyber security is Security operations, automation, and response (SOAR) technology. SOAR technology aims to tackle three key aspects of modern cybersecurity. These three aspects include threat and vulnerability management (orchestration), automation of security operations (automation), and incident response (response) [34]. Input from internal and external sources can be accepted into the SOAR system, also improving visibility of network events and traffic flows. The system can automatically respond to situations using SOAR and AI, as well as recommending actions to security operations teams. The task of the orchestration function is to combine and coordinate the automated and manual processes of the information system [35].

6 Results and Discussion

Cybersecurity has made incredible progress over the past few decades, and there are solid examples of how AI has been applied to it. The results of this study show that AI techniques are suitable for cybersecurity. Integrating AI into security and surveillance systems can increase the effectiveness of anomalies and threat detection. It also reduces the number of daily repetitive tasks that work security teams have to perform.

Before adopt an AI technique, companies should assess their current systems to see what problems they face. There were recurring themes in this research that emerged from multiple sources, and most of these issues could be resolved or mitigated using AI techniques. But the term "AI" is used both as a commercial ploy and as a promising hypothesis of a panacea for any problem. Certain artificial intelligence techniques such as NDR have shown promising results in security tasks, but these are mostly machine learning techniques that are not as complex as could be possible. For example,

these systems are not intelligent in the sense that they have human-like awareness and knowledge in addressing problems.

Most ML techniques still rely heavily on manual oversight and human interaction. The unsupervised learning techniques have the potential to learn on their own, whereas supervised techniques are limited to certain tasks in the security architecture. The aspirations for a self-learning and decision-making computer have been partially satisfied by unsupervised methods and deep learning techniques, and as previously said, DL techniques have elevated the field of AI to a whole new level.

Future work on AI in cybersecurity should allocate more resources to testing unsupervised methods. It's important to remember that artificial intelligence is still a tool for security teams, not a replacement for human reasoning and problem-solving skills. This can improve the Preventive and automated aspects of security systems, so it is important to further develop AI techniques that understand context.

The AI techniques used in attacks may be more sophisticated than defense, so the challenge going forward will be keeping up with the latest techniques from attackers. Most datasets used to train and test AI systems are not up to date and do not contain enough malicious data points. In order for the chosen AI system to be able to learn what a typical activity actually looks like, and vice versa, the dataset needs to be updated [36]. AI techniques can also be compromised, so it is important to protect the integrity of AI techniques. Compromised data collection combined with compromised AI techniques can lead to erroneous results and prevent security systems from functioning properly [37].

Advances in cybersecurity are driven by knowledge and expertise in the field. These talented workers are in great demand and there is a skill gap in cybersecurity. More people need cybersecurity education and training to create identification systems, improve AI techniques, and develop security measures [38]. This is related to the interpretability of AI features, as the analyst needs to understand how the AI component of the system reaches its conclusions. Developing improved AI also requires a basic understanding of current AI techniques, but progress is hampered by widespread ability deficits. By making AI security solutions intuitive to use and visually compelling for companies and enterprises will adopt AI security solutions on a larger scale. The term "AI" is so widely used that there can be confusion about what a particular AI feature actually does. AI-controlled machines are different from AI-enabled machines.

Fully automated AI-driven solutions are still a concept of the future. The primary goal of most AI solutions is to help analysts make better decisions. Industry standards can be established to measure system autonomy and evaluate AI systems to prevent blind reliance on vendor solutions [37]. Product testing transparency is another issue when implementing AI. There may be human resistance to the paradigm shift towards AI, as there are not many industry norms and standards to rely on.

7 Conclusion

The concept of using AI techniques to defend against future cyberattacks has its pros and cons. As attackers and malicious actors continue to improve their attack methods, there is an urgent need for action. IDS, IPS, SOC, and SOAR systems in use today still rely heavily on human intervention. But with the number of attacks outstripping the effectiveness of traditional reactive rule-based defense techniques, the use of AI technology is the ideal way. AI, especially machine learning (ML), gives detection and response systems the opportunity to be more proactive and form real-time actions. It also improves the collection and analysis of network traffic data to improve the effectiveness of security operations and security teams. Today's AI tools are only useful for a limited number of network and cybersecurity related activities. Future research should focus on ways to facilitate automation of AI solutions while reducing the need for human interaction. Achieving this goal requires more accurate assessments, training datasets, and industry standards. ML and DL techniques also need to better understand the context within datasets in order to make decisions similar to humans and have a low rate of false outcomes.

References

[1] K. Thakur and A.-S. K. Pathan, Cybersecurity Fundamentals: A Real-World Perspective. CRC Press is an imprint of Taylor & Francis, 2020. Available: https://tinyurl.com/3kc6v6f8.

[2] "Cyber Security Education: Principles and Policies," Routledge & CRC Press, 2020. https://tinyurl.com/3dy44cua (accessed Apr. 15, 2023).

[3] D. Edeh, "Network Intrusion Detection System using Deep Learning Technique," www.utupub.fi, Aug. 2021, Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/ywhvx2sy.

[4] "Computer Security Fundamentals, 3rd Edition | Pearson IT Certification," www.pearsonitcertification.com, 2016. https://tinyurl.com/4sx2xsdd (accessed Apr. 15, 2023).

[5] D. Franke, "Amazon.com: Cyber Security Basics: Protect your organization by applying the fundamentals: 9781522952190: Franke, Don: Books," Amazon.com, 2023. https://www.amazon.com/Cyber-Security-Basics-organization-fundamentals/dp/1522952195.

[6] C. Sjöblom, "Artificial Intelligence in Cybersecurity and Network security," 2021. Available: https://www.doria.fi/bitstream/handle/10024/181168/sjoblom_christoffer.pdf

[7] R. Mark and R.-O. Bsc, 2022. Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/mr2a9myf

[8] S. A. Salloum, M. Alshurideh, A. Elnagar, and K. Shaalan, "Machine Learning and Deep Learning Techniques for Cybersecurity: A Review," Advances in Intelligent Systems and Computing, pp. 50–57, 2020, doi: https://doi.org/10.1007/978-3-030-44289-7_5.

[9] E. Fossey, C. Harvey, F. Mcdermott, and L. Davidson, "Understanding and Evaluating Qualitative Research," Australian and New Zealand Journal of Psychiatry, vol. 36, no. 6, pp. 717–732, Dec. 2002, doi: https://doi.org/10.1046/j.1440-1614.2002.01100.x.

[10] Rev, "How to Analyze Interview Transcripts in Qualitative Research," Rev, Mar. 30, 2022. https://www.rev.com/blog/transcription-blog/analyze-interview-transcripts-in-qualitative-research.

[11] G. Fernandez, Deep learning approaches for network intrusion detection, M.S. thesis, Dept. Comput. Sci., Univ. Texas at San Antonio, San Antonio, TX, USA, 2019. https://tinyurl.com/3p32m3xt.

[12] P. Uppamma and S. Bhattacharya, "Deep Learning and Medical Image Processing Techniques for Diabetic Retinopathy: A Survey of Applications, Challenges, and Future Trends," Journal of Healthcare Engineering, vol. 2023, pp. 1–18, Feb. 2023, doi: https://doi.org/10.1155/2023/2728719.

[13] J. Li, "Cyber security meets artificial intelligence: a survey," Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, Dec. 2018, doi: https://doi.org/10.1631/fitee.1800573.

[14] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, Jan. 2016, doi: https://doi.org/10.1016/j.jnca.2015.11.016.

[15] "Gmail," accounts.google.com, 2019. https://tinyurl.com/4prmaw9c (accessed Apr. 15, 2023).

[16] K. Corrie, "Building a Large Scale Machine Learning Based Anomaly Detection System Part 2 Normal Behavior of Time Series Data," www.academia.edu, 2019, Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/yc34t6ac.

[17] K. Corrie, "ULTIMATE GUIDE TO BUILDING A MACHINE LEARNING ANOMALY DETECTION SYSTEM PART 1: DESIGN PRINCIPLES," www.academia.edu, 2019, Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/mswk4br8.

[18] J. Huang, Z. Kalbarczyk, and D. M. Nicol, "Knowledge Discovery from Big Data for Intrusion Detection Using LDA," IEEE Xplore, Jun. 01, 2014. https://ieeexplore.ieee.org/document/6906855 (accessed Apr. 15, 2023).

[19] M. Amrollahi, S. Hadayeghparast, H. Karimipour, F. Derakhshan, and G. Srivastava, "Enhancing Network Security Via Machine Learning: Opportunities and Challenges," Springer Link, 2020. https://tinyurl.com/bddar2tx (accessed Apr. 15, 2023).

[20] I. Humied, Cybersecurity Amazon, 2023. Accessed: Apr. 15, 2023. [Online]. Available: https://a.co/d/44cfZbK.

[21] R. Bhardwaj, "IDS vs IPS vs Firewall - Know the Difference - IP With Ease," ipwithease.com, Sep. 10, 2020. https://tinyurl.com/24pxy4jx (accessed Apr. 15, 2023).

[22] N-able, "Intrusion Detection System (IDS): Signature vs. Anomaly-Based," N-able, Mar. 15, 2021. https://tinyurl.com/37de7vn9 (accessed Apr. 15, 2023).

[23] C. Snyder, "NDR vs. IDS for Intrusion Detection - ExtraHop | ExtraHop," www.extrahop.com, Jan. 23, 2019. https://www.extrahop.com/company/blog/2019/network-detection-response-vs-intrusion-detection-systems/..

[24] C. Snyder, "NDR vs. IPS for Intrusion Prevention, Detection, and Response - ExtraHop | ExtraHop," www.extrahop.com, Feb. 07, 2019.

https://www.extrahop.com/company/blog/2019/network-detection-response-vs-intrusion-prevention-systems/ (accessed Apr. 15, 2023).

[25] "NDR and the SOC Visibility Triad | ExtraHop | ExtraHop," www.extrahop.com, 2021. https://tinyurl.com/5n8ejpek (accessed Apr. 15, 2023).

[26] "Point of View." Available: https://www.crowdstrike.com/wp-content/uploads/2021/05/soc-triad-solution-brief.pdf

[27] Nettitude, "The SOC Visibility Triad – SIEM, EDR & NDR | Nettitude," blog.nettitude.com, 2020. https://tinyurl.com/mvuy4mme (accessed Apr. 15, 2023).

[28] I. Cybersecurity Inc., "Dynamic detection for dynamic threats," www.ironnet.com, 2020. https://tinyurl.com/5n89rews (accessed Apr. 15, 2023).

[29] "What is Network Detection and Response?," www.ironnet.com, 2021. https://tinyurl.com/37cct6mh (accessed Apr. 15, 2023).

[30] K. Bissinger, "Darktrace Immune System. Self-learning Detection & Response,"2020. https://tinyurl.com/yzr7u6z4 (accessed Apr. 15, 2023).

[31] K. Bissinger, "Fighting Ransomware with AI," www.n3t.com, 2022. https://www.n3t.com/about-us/blog/fighting-ransomware-with-ai (accessed Apr. 15, 2023).

[32] TechTerms, "SMB (Server Message Block) Definition," techterms.com, 2021. https://tinyurl.com/3mnsa2ft (accessed Apr. 15, 2023).

[33] "About Vectra - AI Driven Cybersecurity Company | Vectra AI," www.vectra.ai. https://tinyurl.com/bhxe967t (accessed Apr. 15, 2023).

[34] FireEye, "What Is SOAR? | Definition & Benefits | Trellix," www.trellix.com, 2019. https://tinyurl.com/muzap5zh (accessed Apr. 15, 2023).

[35] Y. Bari, "Infosys Knowledge Institute | The Future of Tomorrow: Automation for Cybersecurity," www.infosys.com, 2019. https://www.infosys.com/iki/perspectives/future-tomorrow.html (accessed Apr. 15, 2023).

[36] E. Segal, "The Impact of AI on Cybersecurity | IEEE Computer Society," Computer.org, 2020 https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity.

[37] P. Donegan, "'Trusted Research, Analysis and Insight in IT & Telecom Security' AI in Cyber Security: Filtering out the Noise," 2019. Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/ycx5nvwj.

[38] Vectra AI, "E-book Prevention Phase Active Phase Clean-up Phase Initial Infection Minding the cybersecurity gap," 2017. Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/nbjrremc.