Artificial Intelligence for Cybersecurity in Computer Systems and Networks

Authors Names

Mohammed Hasan Hadi[a]

Asmaa Ali Jasim[b]

Publication date: 30 / 8 /2024

Keywords: Artificial Intelligence, Cybersecurity, Computer Systems, Networks

ABSTRACT

The complexity of cyber threats and network assaults is increasing on a daily basis. The worldwide incidence of everyday assaults is increasing, and the methods and strategies used to breach corporate networks and personal devices are varied. The assaults might be attributed to individuals acting alone, organized collectives, or even whole governmental entities. The resources available for conducting assaults are expanding, and as a result, cyber attacks now have the potential to have significant and far-reaching impacts and repercussions. These elements converge to provide challenges for security teams in keeping up with the rapid pace, necessitating the need for more intelligent solutions.

This thesis provides a comprehensive examination of the use of artificial intelligence (AI) techniques, including sub-domains like machine learning and deep learning, to address cybersecurity challenges. This thesis also seeks to demonstrate the use of current AI technologies and their enhancement of cyber security. AI may enhance security systems by enabling them to be more anticipatory and proactive in identifying and addressing threats. Additionally, AI can streamline security operations by automating repetitive processes, therefore saving time. This thesis included conducting interviews with personnel of If insurance firm that specialize in network monitoring and network security. The interviews aimed to ascertain the specific challenges they experienced in their assignments. In this study, potential artificial intelligence (AI) solutions for the identified difficulties are provided**.**

1. Introduction

Computers are indispensable and hard to replace in modern workplaces and daily lives. There is a rising need for information security measures as our technological capabilities develop and expand. There is an enormous amount of data gathered constantly by apps in the business, military, finance, healthcare, and government sectors. Because of this, cybersecurity is very important. We must constantly face and create solutions to the problem of cybersecurity, which is a popular phrase in the field [1].

Data and information security on networks, smartphones, desktops, and other electronic devices or connections is known as cybersecurity, computer security, or information technology security. Assuring the data's availability, confidentiality, and integrity while safeguarding it against harmful assaults, unauthorized access, and other forms of damage are the primary objectives [2].

The majority of cybersecurity measures in use today are rule-based. The process of instructing a computer system on how to process, store, and organize data is known as a rule-based system. In most cases, updates allow the inventor or vendor to modify the rules that are already in the system. In the event of an attack, the system will consult the set of rules to determine how it should respond. We have to turn off and pause the system if we don't have any plans to deal with a specific incursion [3].

The aforementioned issues may be addressed by using AI into cybersecurity. More and more, in the previous decade, we have seen the fast development and widespread usage of cybersecurity systems built on top of artificial intelligence. These solutions may be scaled up to improve cybersecurity by making tasks more efficient and lowering the danger of breaches [4].

[a] Open Educational College , Ministry of Education , Baghdad , Iraq E-Mail: mohammed.almaawi.iq@gmail.com

[b] Open Educational College , Ministry of Education , Baghdad , Iraq E-Mail: a0740551@gmail.com

2. The aim of the study

The overarching goal of this study is to provide evidence that algorithms and systems powered by AI can improve network and cybersecurity. There are many facets of artificial intelligence that this study does not attempt to address. Due to the large variety in both the quantity and nature of assaults, it would be impossible to cover every possible kind of attack and how to fight them all here. Reviewing current technologies and researching their potential applications to network security is the primary objective. Intrusion detection systems are becoming better at seeing and modifying suspicious activity and potential assaults as a result of the increased use of AI techniques in computer security.

3. Literature Review

3.1 Definition of Artificial Intelligence

In recent years, the phrase "artificial intelligence" has entered the vernacular of almost every sector of our society. There is now significant confusion about what exactly AI is due to the word's widespread use. The following definitions should provide a very thorough comprehension of the topic for the next thesis, and the list of definitions is rather extensive. The field known as "Artificial Intelligence" focuses on the calculations that enable perception, reasoning, and action. To put it simply, it's the study and practice of engineering and science that goes into making computers and other electronic devices that can think and act like humans [6].

3.2 History of Artificial Intelligence

The exact roots of artificial intelligence are difficult to identify, although the earliest demonstrations of AI's key concepts may be dated back to the 1940s. During this decade, Isaac Asimov created fictional robots with human-like intelligence and decision-making abilities. Similarly, in the same decade, English mathematician Alan Turing developed The Bombe, which is a more applicable example [5].

During WWII, this device—sometimes called the first computer—cracked and deciphered the German Enigma code. In a subsequent paper, Turing detailed his procedures for evaluating computers' intelligence, which served as a foundation for modern AI. We saw the first computer programmer that could understand and interpret natural English sometime between 1964 and 1966. Eliza was a programmer that could mimic human speech and act out a conversation just like a real person [6].

Coincidentally, that same period saw the invention of primitive problem-solving computer programmers that could automate the solution of some games like Towers of Hanoi. Artificial intelligence and related research received financing in the 1970s as a result of the field's triumphs. Some people were against the ever-increasing investments in AI. Those who argued against expanding AI's capabilities said that computers would never be able to mimic human intelligence [6].

The primary obstacle impeding the advancement of AI initially was the manner in which the human behavioral component was included. The first strategy was constructing a hierarchical structure resembling a stack for the purpose of decision making, using numerous if-then expressions [7]. Rule-based systems, such as expert systems, are effective in certain contexts like chess and other games. In fact, in the 1990s, a computer effortlessly defeated the World Chess Champion [7].

The further advancement in AI was the ability to analyze and assimilate external data, acquire knowledge from it, and adjust to the dynamic working environment. The above statement offers a general explanation of the current understanding of artificial intelligence. Consequently, the earlier

instances from the 1960s and 1970s do not accurately depict the concept of AI as it exists in the present day.

In 2015, Google released AlphaGo, a computer programmer specifically intended for playing the game Go, marking a significant milestone in AI technology. AlphaGo used the processing capacity of machine learning and neural networks to triumph over the top Go players globally, and it continues to be regarded as one of the most advanced AI programmers [8].

3.3 Definition of Cybersecurity

As stated by the Cybersecurity & Infrastructure Security Agency (CISA) cybersecurity refers to the process of safeguarding networks, devices, and data against unauthorized access or illegal exploitation. It involves guaranteeing the confidentiality, integrity, and availability of information. Recently, there has been an increased emphasis on cybersecurity in business due to heightened awareness among consumers and corporations of the risks associated with their confidential information [14].

Furthermore, the implementation of regulatory measures such as the General Data Protection Regulation (GDPR) during the year 2016 and the Data Protection Act (DPA) in 2018 has established explicit guidelines and penalties to incentivize organizations to establish a robust cybersecurity framework and administration. Cybersecurity covers several forms of security [15].

This encompasses "network, endpoint, application, data, cloud, and mobile security". Hence, comprehensive cybersecurity solutions must include the whole system and architecture, rather than only prioritizing the most critical components. As stated before in this section, the fundamental elements of cybersecurity and information security as a whole are confidentiality, integrity, as well as availability. The collection of characteristics is often referred to as the CIA Triad [16].

3.4 Types of Cybersecurity

The primary goal of application security is to safeguard its functionality and assure their implementation in a manner that shields them from potential threats. Software upgrades and testing are methods used to bolster the security of the programmer. Web applications have been identified as the primary area of cybersecurity with the highest number of breaches in recent research. Testing is crucial for maintaining application security and should be conducted regularly during the application's existence [17].

The typical stages of an application's lifecycle include development, quality control, and production. Although organizations often do thorough testing and vulnerability checks in the first and intermediate stages, the true issues arise at the production stage. Conducting ongoing testing beyond the production phase is crucial to sustain the integrity of application security. Given that a significant quantity of our data and information is housed in digital settings, such as cloud storage, safeguarding these storage spaces is as crucial to securing any physical storage units [18].

The majority of attacks against cloud systems exhibit similarities to the aforementioned security categories. Implementing security measures in cloud settings is challenging owing to their unique properties. Cloud services depend on virtual machine solutions, which are susceptible to a range of assaults, including data breaches and Denial of Service (DoS) attacks. Ensuring cloud security requires the vital protection and separation of these platforms. A service injection attempt is another kind of cloud

service attack. In this scenario, the assailant introduces a malevolent input into the system, therefore modifying the operation of a command [19].

Endpoint security is the last area of cybersecurity to discuss. Endpoint security refers to the proactive measures taken to safeguard the network's entry point from potential exploitation or attacks. When we refer to end- and entry points, we are talking about a range of devices including laptops, mobile phones, printers, desktops, smart watches, and any other "smart" item that may be connected to a network. Endpoint security is a well-established concept, but it is sometimes neglected [20].

Currently, the typical antivirus programmer may not be enough to handle the intricacy of hostile threats faced on a daily basis. Data is the most precious resource in the majority of markets and enterprises, necessitating the existence of solutions to safeguard it. Given that networks might have hundreds of access points, the use of automated detection systems and endpoint protection platforms (EPP) is essential to keep up with the rapid pace of technological advancements [21].

4. How Artificial Intelligence Improves Cybersecurity

AI technologies has computational and analytic capabilities that surpass the processing speed of the human brain. Artificial intelligence may provide much faster detection speeds compared to existing approaches. Furthermore, the ability to swiftly detect potential dangers is enhanced, enabling prompt detection of unfamiliar assaults and the development of appropriate reaction strategies in the absence of a pre-existing protocol. Human mistakes continue to be a significant factor in cybersecurity incidents [22].

By applying artificial intelligence (AI) technology, the number of instances caused by human error might be significantly decreased. Artificial intelligence may be used not just for routine, repetitive operations performed on a daily basis, but also for decision-making processes. When making judgements, the use of AI algorithms allows for the testing of data and software, which may help in identifying any overlooked faults and hidden security threats at an early stage [23].

While artificial intelligence may possess superior computational capabilities, it is humans who continue to excel in creative thinking and creativity. Hence, it is advisable to use AI technologies in jobs that are monotonous and repetitive. This allows security personnel to allocate more time to innovative thinking and enhancing the procedure itself [24].

4.1 Cybersecurity Threat Landscape

The yearly threat landscape study by the European Union Agency for Cybersecurity (ENISA) outlines the top 15 cybersecurity risks for 2019 and 2020. The 15 types of assaults include web-based attacks, phishing, web application attacks, malware, spam, ransomware, identity theft, data breach, DDoS, insider threats, cyberespionage, botnets, information leakage, crypto jacking, and physical manipulation, damage, theft, and loss [12].

Among the 15 risks, phishing, information leakage, ransomware, insider threat, and identity theft had an upward trend between 2019 and 2020. In contrast, there was a decline in spam, DDoS attacks, and botnets throughout the same period. The paper identifies two primary causes that contributed to the variations and shifts in the threat environment. Initially, the emergence of the COVID-19 pandemic compelled organizations, enterprises, and nations worldwide to swiftly adjust to a new working environment, which subsequently presented its own set of fresh difficulties [19].

The primary objective of assaults remains focused on achieving financial advantage. Attacks have more dispersion, broader reach, and briefer duration, but provide a more extensive influence. As previously stated, and also indicated in the study [22], a significant proportion of cybersecurity events remain undetected and the time taken to respond to these incidents is too protracted, resulting in an inability to effectively address the increasing number of assaults [20].

4.2 Types of Threats

There are multiple types of security threats that can be defined and classified as follows:

4.2.1 Web-based attacks

The proliferation of web-based services worldwide presents an enticing potential for malevolent individuals to exploit. Web-based attacks include injecting malicious scripts or fake URLs to redirect visitors to a targeted site [26]. This technique may also be used to trick the target into downloading malicious files and injecting hazardous material into websites that are considered trustworthy but have been hacked. A surge of login requests using passwords and usernames, such as brute-force assaults, negatively impacts the fundamental aspects of cybersecurity, including the availability of websites and the confidentiality and integrity of the information available via online services [24].

4.2.2 Malware

Malware is a frequently used technique in cyber criminal activities. Malware refers to harmful software that is specifically designed to carry out activities such as identity theft, cyber espionage, as well as system disturbances. Malware manifests as viruses, Trojan horses, and ransomware . Unlike a conventional bug, malware is intentionally created to do damage [18].

There has been a transition in the use of malware, moving from targeting consumers to targeting businesses. Additional figures indicate that 50% of malware assaults were specifically intended to pilfer personal information, while 71% of targeted firms saw the propagation of dangerous software among their staff. Malware-as-a-Service (MaaS) is a concerning new trend in the field of malware. Unlike Software-as-a-Service (SaaS), Malware-as-a-Service (MaaS) is an illicit industry where criminals engage in the sale and rental of malicious software to other criminals. This empowers anyone without technological expertise to carry out cyber assaults. The accessibility of launching attacks via MaaS organizations has resulted in a rise in botnets [10].

4.2.3 Phishing

The COVID-19 outbreak led to a significant surge in phishing assaults. According to ENISA's research [28], there was a 667% increase in the number of phishing schemes over a one-month period. Emails are the most common medium via which phishing assaults are seen. The email is designed to seem credible, but it really includes harmful files and connections. These emails attempt to exploit human emotions and manipulate individuals into making mistakes as a result. To do this, the perpetrator utilizes phrases like "payment" to elicit hasty and unwise actions from the target. The epidemic has created a general sense of uncertainty and anxiety, which has provided hackers with a significant opportunity to efficiently exploit individuals [17].

In certain cases, criminals use email communication to deceive others by impersonating reputable organizations like the World Health Organization or national health organizations, with the intention of causing damage. Enclosed documents. The practice of remote working has also posed challenges in the

realm of preventing phishing schemes. Microsoft software applications are used in almost every corporation and institution. Phishing attacks sometimes include the use of deceptive emails that contain false error warnings and bogus upgrade recommendations [16].

By using artificial intelligence, it becomes feasible to mitigate issues via the use of pattern recognition and learning capabilities. For example, AI has the ability to identify common patterns in conversations, distinctive traits of interactions, and irregularities in language and syntax. Additionally, it can analyze graphics that are included in emails to identify fraudulent links and login requests [23].

4.2.4 Web Application Attack

The use of the internet has resulted in an increase of web apps, which are crucial for organizations to provide services. Web applications are highly dependent on databases, which are responsible for storing and communicating the required data to the user. Common techniques used to compromise databases include SQL injections (SQLi) as well as cross-site scripting (XSS). SQLi attacks use holes in online security by inserting malevolent code into database queries, therefore obtaining unauthorized access to data and causing detrimental alterations. XSS attacks operate on the same concept, whereby the malevolent code is inserted into web apps and websites, thereby leading the end client to malicious websites [5].

4.2.5 Data Breach

A data breach refers to an occurrence in which unauthorized access is gained to data and/or components of an information system. After successfully infiltrating the compromised system, the attacker has the ability to exploit and obliterate the data. The correlation between data breaches and human mistakes is strong, since many instances of data vulnerability and inadvertent data disclosure may be attributed to inadequate system installation and setup. The complexity of the techniques used by cybercriminals has resulted in a significant number of organizations and enterprises being oblivious to the occurrence of a data breach. Furthermore, apart from the novelty of the crimes, there may be a lack of visibility and categorization inside systems that hinders their ability to identify ongoing attacks. IBM's analysis reveals that the average duration to detect and control a breach is around 208 days, with an average total cost of $3.86 million [14].

4.2.6 Distributed denial of service (DDoS)

DDoS, or Distributed Denial of Service, refers to the situation when a user is unable to access confident data or resources inside a system. In order to do this, the assailants inundate the host network or target with a barrage of requests and traffic, causing the system to fail due to its inability to react. DDoS assaults are a well-known phenomenon to cyber security specialists, but, the methods used by unscrupulous individuals are growing more sophisticated. Analysis of DDoS attack patterns reveals that more than 50% of the assaults have a duration of less than 15 minutes, and these attacks use many attack channels simultaneously [3].

5. Artificial Intelligence Algorithms in Cybersecurity

Artificial Intelligence and cybersecurity have emerged as highly discussed subjects in the current digital environment. As technology rapidly progresses, so do the dangers that exist in the digital realm. Businesses and people are confronted with daunting obstacles in safeguarding their sensitive information, ranging from sophisticated spyware to persistent hackers [15].

5.1 Machine Learning & Deep Learning

When discussing artificial intelligence, we are referring about a vast domain including several subfields of technology. In recent decades, AI has tremendously profited from advancements in deep learning (DL) as well as machine learning (ML) technologies. ML technology, a subset of AI, allows computer systems to acquire knowledge from existing data. Subsequently, the ML application utilizes this data to acquire knowledge and generate its own solutions and methodologies, without the need for explicit programming [21].

Distinct machine learning tasks including classification, regression, and grouping. Classification is the process of categorizing each data point or object into a specific category. For example, in the field of image recognition, the machine learning algorithm is provided with images of two different sorts of objects and its objective is to classify them into two distinct groups. Binary classification refers to the process of categorizing data into two distinct categories, whereas multiclass classification involves categorizing data into more than two categories [13].

Machine learning algorithms may also be used in prediction jobs. Regression refers to the process in which an algorithm is used to forecast a numerical value for an object. Regression may be exemplified by the forecasting of stock prices. The ability to make predictions is facilitated by training the algorithm to recognize and understand particular relationships among the given data points. The accuracy of the prediction is assessed by the magnitude of the discrepancy between the anticipated value and the real value [2].

Clustering techniques are valuable for handling extensive data sets. Clustering refers to the process of categorizing data into clusters, which are groupings that share similarities or have homogeneous characteristics. The distinction between clusters may not always be evident, but the primary objective is to group data points that are more similar to each other in one cluster, and those that are different in another cluster. In order to achieve effective classification, regression, and clustering, it is necessary to decrease the dimensionality of the input data [22].

Deep learning (DL) is a specific branch of machine learning (ML) that utilizes artificial neural networks (ANN) to make judgements. An artificial neural network is a computational model designed to imitate the structure and functioning of the brain of humans, which is a biological neural network. Neurons, which are the individual cells in the brain, are interconnected and communicate with each other via synapses. Artificial neural networks (ANNs) use linked neurons, which are often referred to as processing units. The input to a processing unit might originate from either an external source or the output of another unit. The output from the units may be sent to other units or looped back to the originating unit. The relationship between units and the manner in which information is altered inside the network is contingent upon the weight [6].

5.2 Machine learning approaches

Machine learning methods used in the field of cybersecurity are an effective and influential instrument. Computer systems may improve their performance and develop execution models based on prior data by acquiring the capacity to learn. It can be performed in the following approach :

5.2.1 Neutral network approach

The neural network (NN) approach is a method used to forecast user behavior inside a system. An NN's primary benefit is in its ability to analyze unfamiliar input that is either vague or lacking precision and autonomously generate a solution model. Furthermore, neural network algorithms exhibit strong performance in the task of data generalization, with their ability to handle imprecise input. Nevertheless, neural networks need initial training.

When it comes to cyber security, it is essential to establish instances of attacks and non-attacks, as well as understand the distinction between them, throughout the training phase in order for the system to function effectively. One application of neural network methods is via the usage of self-organizing maps (SOM). The Self-Organizing Map (SOM) is a kind of artificial neural network that is capable of reducing the dimensionality of high-dimensional data [6].

This means that it can take a dataset with several features and turn it into a simpler representation on a one- or two-dimensional grid. The idea was pioneered by the Finnish scientist Teuvo Kohonen and is sometimes referred to as the Kohonen Map. The Self-Organizing Map (SOM) approach is often used in jobs that need pattern detection and data reduction. SOM constructs topological maps by analyzing the input data, hence exposing hidden structures. A topological map is a graphical depiction of a dataset that selectively displays just the essential information [12].

The SOM has similarities to several clustering approaches. The nodes are arranged in a two-dimensional grid, positioning nodes that have similar characteristics in close proximity to each other. This is accomplished by competitive learning, where the weight vector of the node is compared to the inputs vector, and the node that is most similar to the input vector gets positioned closer to the input vector. The node that best matches the input is referred to as the Best Matching Unit (BMU) [19].

The weight of the remaining nodes in the network is determined by the distance to the BMU. Pachghare et al. (2020) did a research on the use of self-organizing maps in intrusion detection. The research used unannotated packets obtained from actual networks to train the model. The experiment's findings demonstrated that SOM is a very efficient technique for intrusion detection systems, since it has the ability to autonomously identify and classify invasive behavior. Due to the need of labelling the training data before to conducting the experiment, the method was somewhat time-consuming [20].

5.2.2 Support Vector Machines

Support vector machines (SVM) are often used for tasks involving classification and regression. Support Vector Machine (SVM) is a machine learning algorithm that uses an unsupervised learning approach to identify a hyperplane that effectively separates data into two distinct groups. A hyperplane is a straight line that is drawn between the data points within a two-dimensional graph. The data points that are closest to the hyperplane are referred to as support vectors, and they play a crucial role in determining the separation between the two classes [24].

If it is not feasible to position the hyperplane in a two-dimensional space, the data points must be transformed into higher dimensions using a technique known as kernelization. An outstanding characteristic of SVM is its capacity to generalize data regardless of the amount of characteristics. Furthermore, SVM has shown superior performance compared to artificial neural networks (ANN) in terms of scalability and prediction accuracy. In a research conducted by Chen et al. (2019), Support

Vector Machines (SVMs) and Artificial Neural Networks (ANN) were evaluated as tools for intrusion detection [18].

The results of the study indicate that SVMs have many benefits over ANN. Support Vector Machines (SVMs) use the notion of structural risk minimization, whereby the goal is to choose the most straightforward classifier to prevent the creation of too complex boundaries. By using this technique, previously unobserved data may be categorized with more ease. Put simply, we reduce the likelihood of incorrectly organizing the data. Support Vector Machine (SVM) approaches are particularly well-suited for finding global solutions and have the advantage of requiring less parameters compared to Neural Networks (NN). In NN, the number of hidden nodes, function transfers, and hidden layers must be defined [10].

5.2.3 Markov model

A Markov chain is a collection of interconnected states, where the transitions between states are determined by probabilistic values. Put simply, a Markov chain provides information on the probability of transitioning from one state to another inside a system. Markov chains may be used to determine the transition probabilities during the training phase in order to accurately represent the typical behavior of the system for threat detection purposes. Hixon and Gruenbacher demonstrate in their work that it is possible to detect malicious packets by analyzing their transitions in the system using TCP/IP headers [17].

If the transition fails to meet the criteria set during the training phase, it might be classified as an anomaly or a possible danger. The hidden Markov model (HMM) is a method in which the prediction of the hidden state is based on the observation of the symbols emitted by the hidden state. For instance, one may lack direct knowledge of the weather conditions, but by seeing people's attire, one might form a rather precise inference about the prevailing weather Various research have explored the use of Hidden Markov Model (HMM) approaches for intrusion detection. Mahoney and Chan developed a technique called packet header anomaly detection (PHAD) for identifying abnormal packet headers. The research demonstrated that the system was able to acquire typical behavioral patterns in various network levels via the use of HMM techniques [16].

5.2.4 Clustering Technique

Clustering techniques include the fundamental concept of categorizing data into clusters based on the similarities and dissimilarities between two occurrences. In order to form clusters, a set of predetermined points that accurately reflect the characteristics of the cluster, known as representative points, are chosen. When a new instance is introduced, its closeness to the associated representative points is used to decide which cluster it belongs to. There are two primary methods for detecting anomalies [23].

The first methodology used unannotated data including both regular network traffic and malicious attack traffic during the training phase. In order for this approach to be effective, it is necessary to assume that abnormal traffic represents just a little proportion of the overall data. By observing the clustering of the data, we may infer that the larger clusters correspond to regular network activity, whereas the smaller clusters, which deviate from the norm, indicate instances of assaults. The second strategy involves only using typical traffic as input during the training step, resulting in the creation of a model that represents normal behavior [11].

5.2.5 Decision trees

Decision trees are a frequently used technique in machine learning for the purposes of categorization and prediction. This approach may be used to estimate discrete functions by categorizing data using a predefined set of criteria. The decision tree consists of three fundamental elements: nodes, arcs, and leaves. The nodes are assigned labels based on characteristics that divide the properties of the node. The arc emanating from the node is annotated with a property that indicates the subsequent action. The ultimate phase entails a leaf that is marked with a class or category. Decision tree algorithms may be used to identify Denial of Service (DoS) and injection attacks. In their study, Vuong et al. (2021) introduced the use of decision trees for identifying and preventing assaults on autonomous vehicles [14].

The decision tree was constructed using characteristics of Denial of Service (DoS) and injection attacks. Furthermore, alongside cyber attributes like network traffic, the physical characteristics of the vehicle, like speed, power consumption, and vibration, were also considered. The findings demonstrated that assaults had distinct effects on cyber attributes and physical attributes. The inclusion of the physical characteristics in the equation resulted in a higher level of accuracy in detecting attacks. In their study, Moon et al. (2022) investigated the use of decision trees in intrusion detection systems as a means of mitigating advanced persistent threats (APT). An Advanced Persistent Threat (APT) is a highly sophisticated kind of cyberattack in which the perpetrators want to infiltrate a network without being detected and maintain a covert presence for an extended duration [9].

In their study, Moon et al. (2023) examined Advanced Persistent Threat (APT) assaults that have the ability to modify their behavior after they have infiltrated the network. They suggested using decision trees as a means to analyze the system's behavior. The decision tree might detect the occurrence of an intrusion based on the observed behavior of the system. The suggested technique achieved a detection accuracy of 84.7%, which is considered high for APT detection [15].

5.3 Deep learning approaches

ML and DL have several similarities, but their primary distinction lies in the process of feature selection. In deep learning (DL), the process of feature selection is automated, in contrast to machine learning (ML) where the selection must be performed manually. The objective of DL techniques is to acquire a more profound comprehension of the input data and extract data characteristics that are beyond the capability of human detection [21].

5.3.1 Deep Belief Network approach

A deep belief network (DBN) is a model that is generated that can visually depict the whole range of potential values in a given scenario. A DBN refers to a collection of restricted Boltzmann machines (RBM) that are arranged in a stacked manner. RBMs are a kind of neural network that can generate probabilistic distributions among a group of inputs. They are composed of a visible layer and many hidden layers [13].

The units within a certain stratum lack interconnectivity . Practically, the concealed layer of the preceding RBM functions as the observable layer for the subsequent group of RBMs, and this process continues until every single layer of the DBN are trained. One important feature of a DBN is that every RBM layer is taught to have knowledge of the full input, allowing the network to effectively identify patterns in the data. The optimization and categorization of the patterns obtained during the training phase requires just a limited amount of labelled data, which confers a performance benefit [8].

5.3.2 Recurrent neural networks

Recurrent neural networks (RNN) are a category of artificial neural networks that are designed to process and analyze data sequences. In contrast to a unidirectional feed-forward network (FNN), a recurrent neural network (RNN) enables bidirectional signal propagation by including loops inside the network. RNN incorporates loops to provide memory retention, enabling it to store and use information from past occurrences, hence influencing the current input and output. RNN models are well-suited for scenarios where the data patterns exhibit temporal changes and for cases where one seeks to determine the impact of several input factors on the output, which may be used in the field of cybersecurity [6].

5.3.3 Automatic encoder approach

An auto encoder is a kind of neural network that utilizes unsupervised learning. The output layer of auto encoder networks has the same dimensions (number of units) as the input layer. An auto encoder functions by reducing the dimensionality of the input data. The intermediate levels, often known as buried layers, have a reduced amount of units available for processing. This enables the network to reduce noise and extract crucial characteristics of the input. The result is a reconstruction derived from the downsized version in the intermediate layer. An automated encoder generally has three components in its construction [6].

The first element in the network is referred to as the encoder. This fully linked feedforward network transforms the input data by reducing its dimensionality into a latent space representation. The code component is given the compressed form of the input. Subsequently, the data is inputted into a comparable structure to the encoder, known as the decoder. This component performs the inverse operation by reconstructing the data to accurately replicate the input, maintaining the same number of units and dimensions. To comprehend the intrinsic patterns and characteristics of intricate data sets, one may layer auto encoders to form a deeper network. Auto encoders are used in Convolutional Neural Networks (CNNs), Restricted Boltzmann Machines (RBMs), and Deep Belief Networks (DBNs) [12].

Conclusions

Using AI technologies to address future cyber assaults is a concept that has both positive and negative implications. Given the continuous improvement of attack strategies by attackers and malevolent actors, it is imperative to respond promptly. However, there is a little misunderstanding about the true capabilities of AI in the field of cybersecurity. Artificial intelligence solutions are promoted as the ultimate solution to a wide range of security issues, but the industry has not yet reached that level of advancement. Most of the current Intrusion Detection Systems (IDS), Network Detection and Response (NDR), and Security Orchestration, Automation, and Response (SOAR) technologies still heavily rely on human interaction.

Nevertheless, embracing AI technologies is the optimal path to take, since conventional reactive, rule-based preventative methods are inadequate in addressing the magnitude of threats. Modern cyberattacks have the ability to bypass several outdated security measures and remain completely unnoticed, resulting in significant financial and reputational harm to businesses and organizations. Artificial intelligence (AI), particularly machine learning (ML), enhances detection and response systems by enabling them to be more proactive and take real-time responses. Additionally, this enhances the process of gathering and analyzing network data, hence increasing the effectiveness of security operations and the productivity of security teams. Current AI approaches are limited to certain functions within the domains of cyber and network security.

There is a need for more investigation into reducing human engagement and increasing the automation of AI solutions in the future. In order to accomplish this objective, it is necessary to have a greater number of precise examinations, training datasets, and established norms within the business. In order to achieve humanlike decision-making with a low proportion of erroneous outcomes, it is essential for ML and DL techniques to enhance their ability to comprehend context inside datasets. The majority of information on AI products is provided by vendors, which inevitably introduces bias when evaluating the effectiveness of the solution. In the foreseeable future, artificial intelligence (AI) solutions will serve as invaluable tools for security analysts, enhancing the speed and efficiency of data collecting and root-cause investigation operations. It is crucial to bear in mind that achieving a completely automated security infrastructure powered by AI may not be feasible, and this is a key consideration when examining and evaluating the role of AI in cybersecurity in the future.

References

[1] W. Shafik, "Artificial Intelligence and Blockchain Technology Enabling Cybersecurity in Telehealth Systems," Artificial Intelligence and Blockchain Technology in Modern Telehealth Systems, pp. 285–326, 2023.
[2] M. K. Thukral, "Cybersecurity in brain computer interface-assisted hemiplegia rehabilitation: A Blockchain-centric perspective," in 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 2023.
[3] A. Moallem, "Cybersecurity in smart and Intelligent Manufacturing Systems,"Smart and Intelligent Systems, pp. 149–162, 2021.
[4] K. Kaushik, "Blockchain enabled Artificial Intelligence for cybersecurity systems," Studies in Big Data, pp. 165–179, 2022.
[5] R. Luis de Moura, V. N. Franqueira, and G. Pessin, "Cybersecurity in industrial networks: Artificial intelligence techniques applied to intrusion detection systems," in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), 2023.
[6] F. Wahab, A. Shah, I. Ullah, H. Khan, and D. Adhikari, "The significance of artificial intelligence in Cybersecurity," Artificial Intelligence for Intelligent Systems, pp. 105–119, 2024.
[7] W. Shafik, "Artificial Intelligence and Blockchain Technology Enabling Cybersecurity in Telehealth Systems," Artificial Intelligence and Blockchain Technology in Modern Telehealth Systems, pp. 285–326, 2023.
[8] M. K. Thukral, "Cybersecurity in brain computer interface-assisted hemiplegia rehabilitation: A Blockchain-centric perspective," in 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 2023.
[9] A. Moallem, "Cybersecurity in smart and Intelligent Manufacturing Systems," Smart and Intelligent Systems, pp. 149–162, 2021.
[10] K. Kaushik, "Blockchain enabled Artificial Intelligence for cybersecurity systems," Studies in Big Data, pp. 165–179, 2022.
[11] R. Luis de Moura, V. N. Franqueira, and G. Pessin, "Cybersecurity in industrial networks: Artificial intelligence techniques applied to intrusion detection systems," in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), 2023.
[12] F. Wahab, A. Shah, I. Ullah, H. Khan, and D. Adhikari, "The significance of artificial intelligence in Cybersecurity," Artificial Intelligence for Intelligent Systems, pp. 105–119, 2024.
[13] W. Shafik, "Artificial Intelligence and Blockchain Technology Enabling Cybersecurity in Telehealth Systems," Artificial Intelligence and Blockchain Technology in Modern Telehealth Systems, pp. 285–326, 2023.
[14] V. Makoiedova, "Information technology: Approaches to definition, principles of construction," Cybersecurity: Education, Science, Technique, vol. 2, no. 18, pp. 138–149, 2022.
[15] B. Pandey and S. Ahmad, "Cybersecurity exercises and teams definition," Introduction to the Cyber Ranges, pp. 79–94, 2022.
[16] J. Lewallen, "Emerging technologies and problem definition uncertainty: The case of cybersecurity," Regulation & Governance, vol. 15, no. 4, pp. 1035–1052, 2020.

[17] N. Kulev, "Analysis of definition set formed by given definitions of term cybersecurity," Journal of Defence & Security Technologies, vol. 2, no. 0, pp. 3–10, 2020.
[18] N. Karabut, "Cybersecurity approaches to the definition of a concept," in International Scientific and Technical Conference Information Technologies in Metallurgy and Machine Building, pp. 440–444, 2020.
[19] G. Collard, S. Ducroquet, E. Disson, and G. Talens, "A definition of information security classification in cybersecurity context," in 2017 11th International Conference on Research Challenges in Information Science (RCIS), 2017.
[20] H. Danilo Jaramillo, S. A. Cabrera, E. M. Abad, V. A. Torres, and J. C. Verdum, "Definition of cybersecurity business framework based on ADM-TOGAF," in 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), 2015.
[21] D. Rivera, F. Monje, V. A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, and J. Berrocal, "Automatic translation and enforcement of cybersecurity policies using a high-level definition language," Entropy, vol. 21, no. 12, p. 1180, 2019.
[22] S. M. Toapanta, N. A. Peralta, and L. E. Gallegos, "Definition of parameters to perform audit in Cybersecurity for Public One Organization of Ecuador," in Proceedings of the 2019 2nd International Conference on Education Technology Management, 2019.
[23] D. Liszkowska, "Turkey's cybersecurity policy framework," Cybersecurity and Law, vol. 11, no. 1, pp. 79–91, 2024.
[24] E. Hodyr, "Cybersecurity of Air Force," Cybersecurity and Law, vol. 8, no. 2, pp. 56–69, 2022.