Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Proposing Strength, Weakness, Opportunities and Threat (SWOT) Analysis Model for Implementation of Artificial Intelligence in Detection of DDoS Assaults

Anil Suhag[1], Dr Avneesh Kumar,

Galgotias University

Abstract - With the rapid advancements in Information and Communication Technology challenges for cyber security (CySe) have become sophisticated and more lethal. Conventional methods and thought process for cyber security (CySe) are not capable to handle the issue of Cyber Security (CySe) due to human limitations and the fact that cyber assaults are becoming intelligent, sophisticated and complex; therefore, there is a need for new approaches, which are ideal, scalable, adaptable and flexible. The aim of the paper is to carry out Strength, Weakness, Opportunities and Threat (SWOT) analysis of implementation of Artificial Intelligence (ArIn) supported Cyber Security (CySe) techniques in monitoring, detecting, understanding, and then launching counter assaults. This paper deals with the effects of Distributed and Compact Artificial Intelligence (ArIn) methods on cyber threats. It is advantageous if we have the ability to use better Artificial Intelligence (ArIn) methods and technology in Cyber Security (CySe) than one possessed by the adversary. Future directions of research have been discussed for enhancing the employment of Artificial Intelligence (ArIn) advancements in improving Cyber Security (CySe).

Keywords : Cyber Security (CySe), Artificial Intelligence (ArIn), Strength, Weakness, Opportunities and Threat (SWOT)

1. Introduction

Grey Zone Warfare is the norm in the modern day, and the most perilous and lucrative battlefield is cyber space, which is unconstrained by laws or regulations. The growing danger posed by warfare in cyber domain to national security and economy has not been fully understood and recognized. Information warfare, which encompasses all media, components of propaganda, and perception control, includes cyber warfare [1]. Cyber security (CySe) is not only limited to internet, but to every other form of communication. This gap is closing and the threat is rising as connectivity grows and therefore, we can comment that the threat in cyber domain is posing one of the biggest challenges to national security and economy. Cyber security (CySe) is a complicated problem and therefore, needs multi-faceted, multi-layered initiatives and solutions.

Cyber Security (CySe) is adapting to challenges but the threat is still looming large, as assaulters are integrating Artificial Intelligence (ArIn) with large volume assaults. This daunting task of handling large scale assaults has increased the challenge many folds. Accuracy in detection, accelerating the investigation, and automating the response, provides the mechanism of protection to safeguard against threats in cyber domain. Artificial Intelligence (ArIn) has preventative and problem-solving skills, and therefore, data breaches can be avoided efficiently. Artificial Intelligence (ArIn) is required in Cyber Security to protect, detect, mitigate, prevent, respond and predict future cyber assaults [2]. The capability of Artificial Intelligence (ArIn) to learn, understand, act, and improve based on input makes it ideal for integration with Cyber Security (CySe). Moreover, Artificial Intelligence (ArIn) is the subset of Machine Learning (MaLe), Deep Learning (DeLe) and

Neural Networks (NeNe) and Expert Systems and Artificial Intelligence (ArIn) has assisted, augmented and autonomous intelligence. Therefore, we can comment that Artificial Intelligence (ArIn) is essential for Cyber Security (CySe) as complex and sophisticated threats can only be countered by smart protection methods [3].

2014 Data Breach Investigations Report of Verizon indicates that 92% of cyber assaults in the last decade can be pin pointed to just nine very basic cyber assault patterns. The complexity and scale of threats is increasing exponentially with every passing day and this has increased vulnerabilities of the networks [4]. The objectives of cyber assaults and the prominent threat pattern is shown in **table 2**.

Table 1 : Objectives and Assault Patterns

Objectives	**Assault Patterns**
The Loss of Integrity of Data Information is modified	• Control gaining malware • Exploitation of insider or privilege • Physical loss or theft • Assaults on web apps • DoS/ Distributed DoS assaults • Cyber Espionage • Intrusion at the Point of Sale • Payment Card Skimmers • Miscellaneous mistakes like emailing the wrong person
Loss of Availability of Data Crucial data and system are inaccessible to the authorized users	
Loss of Confidentiality of Data Unauthorized users receive access to critical and sensitive information	
Physical Destruction of Data Physical destruction through instructions that cause deliberate malfunctions	

2. Research Objectives

2.1 To perform a detailed Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of implementing Artificial Intelligence (ArIn) in cyber security (CySe) practices.

2.2 To assess various ArIn methodologies, including Distributed and Compact AI methods, to understand their potential impact on monitoring, detecting, and responding to cyber threats.

2.3 To investigate how AI-powered solutions can strengthen cyber defense mechanisms by providing real-time threat intelligence, automating threat detection, and facilitating adaptive response strategies.

2.4 To propose a model for investigating how ArIn can be leveraged not only for defense but also for launching effective counter assaults against cyber adversaries.

3. Layout of the Paper

The paper aims to conduct a Strength, Weakness, Opportunities and Threat (SWOT) analysis of using Artificial Intelligence (ArIn) in detecting, analyzing, and preventing cyber assaults.This paper compares distributed and compact Artificial Intelligence (ArIn) methods for cyber threat detection. It is advantageous to use Artificial Intelligence (ArIn) technology with enhanced features and improved capability. Therefore, research gaps and future directions of research in the implementation of Artificial Intelligence (ArIn) in Cyber Security (CySe) have been discussed. Finally, the conclusion has been presented after evaluating the employment of different Artificial Intelligence (ArIn) methods in improving Cyber Security (CySe) posture. The sections of the research paper are organized as follows: The methodology used for the literature review is described in Section 2, Section 3 deals with comparative study of distributed and compact Artificial Intelligence (ArIn) methods on cyber threats. Section 4 outlines the SWOT analysis of Artificial Intelligence (ArIn) in Cyber Security (CySe). Sections 5 and 6 cover research gaps, scope of future research, and study conclusions.

4. Methodology

4.1 Systematic Approach.

Firstly, the focus was on the selection of search engines and databases for the literature review. Secondly, specific keywords with respect to the topic of research paper were identified. As a third step, we compiled a digital library of literature by downloading articles and research papers that are closely related to the topic. We specifically focused on recent advancements in the incorporation of Artificial Intelligence (ArIn) in Cyber Security (CySe). To do this, we conducted searches on various platforms such as Google, the Google Scholar, Research Gate, and IEEE Xplore to gather relevant articles and papers. Fourthly, all the downloaded articles and papers were studied and then prioritized as per relevance to the topic of the research paper. Eventually, research gaps and future directions of research in the incorporation of Artificial Intelligence (ArIn) in Cyber Security (CySe) were identified.

4.2 Focus on Recent Years.

The literature review focused on the relevance of downloaded articles to the research paper's topic and publication date. The approach is based on the abundance of existing research on the integration of Artificial Intelligence (ArIn) in Cyber Security (CySe). The main reason for this approach is that there are a large number of papers already published on superimposing Artificial Intelligence (ArIn) on Cyber Security (CySe) and to advance this field and identify research gaps and future directions, recent and relevant articles have been consulted. The aim is to contribute to the development of Artificial Intelligence (ArIn) in Cyber Security (CySe).

5. Comparison : Distributed and Compact Methods of ArIn.

Incorporation of Artificial Intelligence (ArIn) in Cyber Security (CySe) allows for the adjustment and adaptation of execution strategies based on recently acquired data. Analyzing previous results, can improve the performance of Artificial Intelligence (ArIn) models. Additionally, it possesses features like tenacity, simultaneity, and tolerance for imprecision, defects, and uncertainty. Artificial Intelligence (ArIn) superimposed on Cyber Security (CySe) provides security professionals with a capability to learn, understand, act and improve on the basis of information fed to the system. Moreover, Artificial Intelligence (ArIn) has assisted, augmented and autonomous intelligence [4]. Also, Artificial Intelligence (ArIn) has Abilities to predict threats on the basis of prior solutions and take assistance of Natural Language Processing (NLP) to analyze unstructured data, provide unique solutions and detailed insight for quick and cost effectively method of stopping intrusions and preventing intrusions even before they occur. The complex and sophisticated threats launched on a mega scale can be countered by the integration of Artificial Intelligence (ArIn) into Cyber Security (CySe) systems [5]. Let us discuss different Artificial Intelligence (ArIn) strategies to predict and prevent digital ambush. We are migrating towards a future in which human resource will collaborate with intelligent machines.

5.1 Distributed Methods

5.1.1 Intelligent Agents (InAg).

The autonomous system consists of multiple Intelligent Agents (inAg) that distribute data and collaborate to respond to unforeseen events [6]. An Intelligent Agent (InAg) is an independent entity that uses sensors to detect movement, actuators to monitor the environment, and directs its activity for achieving goals and objectives. To achieve their goals and objectives, they learn or use knowledge base. It exhibits behaviour like pro-activity, reactivity, and understanding the agent interaction language [7]. They have the capacity to adapt in real time, communicate with their surroundings to learn new things, and have storage with memory and recovery capacities. The comparative study is shown in **table 3**.

Table 3 : Comparative Study : Intelligent Agents

Ref	Method	Environment	Brief of Study
[6]	Multi Agent System (MuAgSy)	Intrusion in wireless sensor network	Node trust value has been used for predicting intrusion
[7]	Multi Agent System (MuAgSy)	Network Intrusion in a cloud environment	Detecting and preventing malicious attacks through the use of Intrusion Detection Systems.
[6]	Adaptive Rule based Multi Agent System (MuAgSy)	Transferring data within a network	Multi-agent rules (MuAgSy) for secure data transfer

5.1.2 Neural Networks (ArNeNe)

Neural networks (NeNe), are composed of interconnected neurons that are designed to detect patterns, associations, and functional dependencies. Neural Networks (NeNe) are well-trained networks with Feed Forward and Back Propagation capabilities that provide more accurate and reliable outcomes. Using information acquired from various users,and audit records over a significant period of time, neurons are effectively trained and educated. Everyday traffic patterns are illustrated, and anomalies are detected and highlighted if an incoming network data exceeds a predetermined threshold given to the neurons. The reconstruction error, which is the difference between the actual and desired output, is commonly used as an anomaly score. It is in a position to recognize and identify both future unforeseen assault patterns and earlier observed assault patterns. Neural networks (NeNe), are time-consuming expensive process, as it takes additional time to gather and analyze training data. The trained data gathered from Deep Learning can identify whether a file is malicious or legitimate without human participation. The neural nets increase speed. The comparative study is shown in **table 4**.

Table 4 : Comparative Study : ANN

Ref	Method	Envt	Brief of Study
[8]	Multiclass cascade of Neural Network (NeNe)	Boosting based Neural Network (NeNe) with Adaboost	Cascade of ensemble based ArNeNe for IDS.
[9]	Deep Learning based Neural Network	Multilayer Feed Forward (FeFo) Artificial Neural Network (ArNeNe)	Deep neural network (NeNe) for IDS. Back Propagation (BaPr) was used.
[10]	Artificial Neural Network	Multilayer Feed Forward Perception (FeFoPe)	Use of ArNeNe for IDS. KDDCUP'99 data set was used.
[11]	Artificial Neural Network	IoT Network	ArNeNe to detect intrusion using Feed Forward (FeFo) and backward learning (BaLe) algorithm.

5.1.3 Artificial Immune Systems (ArImSy)

It is a technique for managing cyber assaults. It simultaneously operates on immune-cell growth (variation, self-tolerance, and clone) and antigen detection. The comparative study is shown in **table 5**.

Table 5 : Comparative Study : ArImSy

Ref	Method	Envt	Brief of Study
[12]	Deep DCA	IoT Network	Dendritic cell method and deep learning used in a hybrid model to reduce false alarms
[13]	Artificial immune system (ArImSy)	Network of nodes	A network of nodes to separate malicious from benign nodes. Bits were used to represent each node.
[14]	Negative selection & danger theory algorithms	IoT Network	Characteristics of an ArImSy based IDS for IoT that are desirable.A layered, hierarchical strategy was adopted.
[15]	Negative selection algorithm and Clonal selection algorithm	IDS	IDS employs NSL-KDL dataset. The ratio of features and detectors to classification accuracy was linear (directly proportional)

5.1.4 Genetic Algorithms (GeAl)

The Genetic Algorithm (GeAl) is an evolutionary algorithm that uses natural selection to find optimal solutions to complex problems. It employs various methods such as inheritance, mutation, selection, and a crossover to mimic natural evolution and generate solutions. The Genetic Algorithm (GeAl) is a heuristic search algorithm that uses tools based on natural selection and eugenics to find approximate answers to optimization problems. The algorithm optimizes the limited resources and provides accurate results. The Genetic Algorithm (GeAI) can extract classification rules from incoming data and select optimal metrics to flag assault traffic. The human element in a feedback loop reduces false positive rates and selects the proper test cases. The algorithm is versatile and robust, making it resistant to noise and changing inputs. A fitness function can be used to improve the system's fitness by combining detection rate, false positives, and the ratio of the reduced training dataset. This requires communication among the agents and a significant training period. GeAl is able to identify cyber assaults with an early detection method that analyzes traffic patterns using evolutionary algorithms and packet-based window sizing [19]. The comparative study is shown in **table 6**.

Table 6 : Comparative Study : Genetic Algorithms

Ref	Method	Envt	Brief of Study
[16]	GeAl	Randomly generated chromosome	IDS using randomly generated 100 chromosomes
[17]	GeAl	FWP-SVM genetic algorithm	FWP-SVM Genetic Algorithm (GeAl) that includes parameter optimization, feature selection, and weighting. The optimization of a cross over and mutation probabilities decreased the SVM error rate.
[18]	GeAl	Signature based IDS	Each and every GET request was transformed into a chromosome.

5.2 Compact Methods

5.2.1 Machine Learning

It involves training the machines that analyze data for learning and taking decisions using algorithms. It relies heavily on mathematical techniques for gathering data, identifying patterns, and drawing conclusions. Machine Learning (MaLe) enables computers and systems to learn and respond to new data, allowing them to perform tasks that were not originally programmed. The focus of Machine Learning (MaLe) is on computer programs that can learn autonomously from massive amounts of data. This technology provides multiple ways to detect network intrusions apart from signature databases. The two main methods of Machine Learning (MaLe) are classification and regression. The comparative study is shown in **table 7**.

Table 7 : Comparative Study

Ref	Method	Envt	Brief of Study
[20]	Naive Bays, SVM, bagged decision trees, random forest, extra trees, AdaBoost, Stochastic gradient boosting	Email filtering : Spam and Phishing	comparison of spam and phishing email filters
[21]	Decision tree, random forest, gradient boosting	Detect phishing	Using feature selection algorithms for phishing website detection
[22]	Logistic Regression	Detect phishing	Assault detection using hyperlinks found in source code of specific websites
[23]	K-means, KNN, Fuzzy, C-means, SVM, Naive Bayes, RBF (Radial basis Function), Ensemble method	Network Intrusion	Comparative study of intrusion detection. RBF outperformed others in accuracy

5.2.2 Expert Systems

A computer programme that simulates human decision-making is known as an expert system. The knowledge base and inference engine respectively represent real-world instances and automatic reasoning systems [24]. It assesses the knowledge base's present state, applies the appropriate rules, and then adds new knowledge [25]. The components of Expert System are shown in **table 8**.

Table 8 : Components of Expert System

Knowledge Base	Malicious and whitelisted IP Addresses,
	Known Malware and virus
	Approved applications
	Data usage at end points
Inference Engine	The Geographical location, connection pattern, and the attempts to IP address
	Login time-stamp and attempts
	Port Communication
	Document & a program access pattern and frequency of usage

5.2.3 Fuzzy Logic

The Fuzzy Logic (FuLo) technique determines mean packet arrival times using a fuzzy estimator. Although it excels at interpreting rules, it cannot learn them automatically and requires assistance. The fuzzy set hypothesis, suggests that reasoning is estimated rather than precisely obtained through traditional predicate logic. It uses both fuzzy sets and rules to handle numerous unclear and incomplete input metrics, such as CPU usage duration, activity rate, and connection interval. To be able to effectively detect and explain security attacks, it incorporates inputs from diverse sources to set if-then rules. By utilizing the mean packet inter-arrival times, the Fuzzy estimators can precisely detect and identify cyber attackers. It provides robust protection against port scans and probes by targeting specific criteria for detection instead of constructing a model to highlight the system's current state. This reasoning, in conjunction with statistical analysis, can be used to accurately and effectively detect cyber attacks [29]. The comparative study is shown in **table 9**.

Table 9 : Comparative Study : Fuzzy Logic (FuLo)

Ref	Method	Envt	Brief of Study
[26]	The Fuzzy based defense mechanism	DDoS in Cloud Computing	To identify and mitigate DDoS, a fuzzy logic-based defence mechanism was used in a cloud environment.
[27]	The dynamic fuzzy rule interpolation	Network Intrusion	Use of the dynamic fuzzy rule interpolation approach to increase system accuracy.
[28]	Fuzzy logic with associative rules	Detecting phishing websites	To identify the nature of the websites by using input features.

6. SWOT Analysis

SWOT analysis of Artificial Intelligence (ArIn) in Cyber Security (CySe) will assist us in identifying the technology's strengths, weaknesses, and areas that require improvement so that we can we can take advantage of the strengths, provide solutions to the challenges, seize new opportunities, and simultaneously manage risk.

6.1. Strength

6.1.1 Quick Detection

Artificial Intelligence (ArIn) has much greater analytical and monitoring capabilities than humans. Threat detection is the first step in cyber defense; it is desirable that un-trusted data is detected at an early stage so as to prevent the network from suffering permanent harm. By fusing Artificial Intelligence (ArIn) with Cyber Security (CySe), risks can be detected in real time as they arise. Artificial Intelligence (ArIn) examines the entire system for any potential dangers. Artificial Intelligence (ArIn) will spot dangers much earlier than humans do, making cyber security quicker and flexible [30].

6.1.2 Fast Response

Unending amounts of data must be examined and reported for data protection. Terabytes of data is quickly fed to artificial intelligence (ArIn) enabled system. The system analyses data and foresees threats [30]. Artificial intelligence (ArIn) is ideal for preventing data breaches before they cause any damage since it gives a faster incident reaction time.

6.1.3 No Human Errors

Using smart and data driven algorithms, Artificial Intelligence (ArIn) can be used to perform daily security tasks of cleaning as well as making crucial strategic decisions. Artificial intelligence (ArIn) is a force multiplier as it manages the knowledge base of recent viral threats by creating intelligent databases, categorizing risks, and then reacting to threats [31]. If correctly harnessed, Artificial Intelligence (ArIn) systems can generate threat alerts, identify new malware strains, and protect important data. Artificial Intelligence (ArIn) systems can be trained to give alarms for threats, identify novel malware strains, and protect crucial data.

6.1.4 Data Analytics

Artificial Intelligence (ArIn) has efficient data analytics skills and hence, can be used to quickly, effectively, and accurately analyze enormous volumes of electronic data. Artificial intelligence (ArIn) can quickly identify both known and unidentified threats through behavioural analysis. Additionally, by anticipating cyber assaults, automated solutions save time and money. Artificial intelligence (ArIn) is also capable of handling unexpected threats and developing response plans from scratch, in contrast to conventional processing methods. Artificial Intelligence (ArIn) constantly examines vulnerabilities in the network and makes critical decisions within seconds without human interaction. Every day, a sizable volume of data is transmitted via a network. This information needs to be protected from malicious software and people. Experts in cyber security (CySe) can't, however, keep an eye on every communication for potential threats [32]. Artificial intelligence (ArIn) is the

finest method for assisting in identifying risks that masquerade as routine behaviour. Due to its automated nature, Artificial intelligence (ArIn) can quickly scan through massive volumes of data and traffic. Data can be transferred with the aid of artificial intelligence based technology, such as a residential proxy [33].

6.1.5 Less Time Consuming

With the assistance of Artificial Intelligence (ArIn), the security experts can devote more effort and time to long term and strategic goals [30]. It makes sense to not involve human experts in readily automated jobs and allow them to concentrate on more critical operations as they are still far superior to machines in terms of creativity and strategic insight.

6.1.6 Prevent Spreading

Utilizing Artificial Intelligence (ArIn) is crucial for detecting interference, as it allows for prompt response to even anonymous threats [30] [31]. AI is a vital component of our solutions, aiding us in swiftly detecting and analyzing new exploits and vulnerabilities to prevent future attacks.

6.1.7 Flexible and Robust

Artificial Intelligence (ArIn) in Cyber Security (CySe) is more flexible, robust and versatile than the existing Cyber Security (CySe) solutions. By guaranteeing a better Cyber Defence system against an increasing number of sophisticated and complicated cyber threats, it improves security. The use of curated risk analysis by Artificial Intelligence (ArIn) shortens the time security analysts need to make important decisions.

6.1.8 Constant Learning.

Artificial Intelligence (ArIn) uses its potential to gradually improve network security. It learns a network's behaviour over time using Deep Learning (DeLe) and Machine Learning (MaLe). It identifies patterns and groups them, thereafter, investigates for irregularities or security incidents and eventually takes appropriate action [33]. The patterns that Artificial Neural Networks (ArNeNe) establish over time can be used to improve security in the future. Potential threats with traits similar to a database are immediately stopped [22]. Assaulters find it challenging to surpass artificial intelligence (ArIn) intelligence since artificial intelligence (ArIn) is constantly learning [34].

6.1.9 Network Centric Environment.

Artificial Intelligence (ArIn) can quickly identify, assess, and respond to cyber assaults in a network-centered environment. Quick decision-making, rapid scenario evaluation, and decision superiority are all possible with Artificial Intelligence (ArIn) driven setup made up of an automated knowledge architecture with lateral and vertical sharing.

6.1.10 Negative Effects

It is essential to create artificial intelligence (ArIn), a system that performs Cyber Security (CySe) without causing any harmful side effects. Artificial intelligence (ArIn) will start becoming smarter and more self-reliant as research continues, eventually replacing humans. As technology advances, ethical and legal concerns arise in the use of technology in cyber forensics [32].

6.1.11 Predict Future Assaults

It is not possible for Humans to identify and detect each and every threat that a network confronts. Moreover, assaulters launch hundreds of millions of assaults using a combination of known and unknown threats. Therefore, it is essential to adopt contemporary solutions to stop assaulters from attempting new strategies, including virus assaults and sophisticated social engineering assaults. Artificial Intelligence (ArIn), is the contemporary solution for mapping and stopping unknown threats [32]. Contrary to previous systems, Artificial Intelligence (ArIn) systems can predict future cyber security (CySe) threats based on past threats, even if those threats change.

6.1.12 Vulnerability Management.

To secure a network, vulnerability management is essential. For a network to be secure, threats must be detected, identified, and then avoided [33]. By identifying vulnerabilities in computer systems and networks, Artificial Intelligence (ArIn) enables security professionals to focus on their core responsibilities.

6.1.13 Cognitive Computing

The next development in artificial intelligence is cognitive computing (ArIn). In the past, computers with artificial intelligence (ArIn) could keep a record of their responses and even the process they used to arrive at those results. But even after coming up with a solution, they didn't actually learn anything. But creating tools that improve human abilities is the ultimate aim of artificial intelligence (ArIn). Instead of just spouting replies, cognitive computing accomplishes things in a different way. Instead, it offers analysis based on its investigation. Additionally, it updates that knowledge when the new data is made accessible. It might eventually reach conclusions that a person would not. Cognitive computing mimics how the human brain thinks [25]. It is capable of learning, information gathering (data mining), pattern recognition, and human language communication. Cognitive computing takes decisions based on the insights provided by the computer .

6.1.14 The Prioritization of Threat

The hackers are altering their strategies on a daily basis, and therefore, the risks and challenges, that network confronts is evolving over time. It becomes challenging to order security tasks as a result. Phishing attacks, denial-of-service (DoS) attacks, and ransom-ware might all occur simultaneously. Although the potential for these assaults is comparable, we must first identify the priority. The bigger dangers that can complicate security are carelessness and human error [36]. Artificial intelligence (ArIn) can be installed on a network to identify all forms of attacks, assist you in prioritizing them, and help you stop them.

6.1.15 Core Security Issues

Assaulters continually alter their modus operandi, but the practices of defender do not evolve and remain constant. Artificial intelligence (ArIn) not only imitates the best practices of security, but also gets rid of their weaknesses and manages the redundant Cyber Security (CySe) procedures. It aids in frequently detecting and preventing core security issues [24]. A thorough network analysis is also carried out to look for security flaws that could jeopardize the security infrastructure.

6.1.16 Learning Methods

Through Machine Learning (MaLe), Deep Learning (DeLe), and Neural Networks, artificial intelligence (ArIn) reduces the susceptibility of networks (NeNe). Artificial intelligence (ArIn) uses these learning techniques interchangeably to improve information security, predict attacks, categorize threats, optimize the data protection process, and quickly produce complete reports. These learning techniques examine a vast quantity of data, identify the dangers, and rank them. This works effectively and saves time and money. Machine learning (MaLe) can operate with full, partial, or no supervision. Using Neural Networks (NeNe), Deep Learning (DeLe), a subset of Machine Learning (MaLe), enables computers to learn on their own, unsupervised (NeNe). Reading unstructured data allows Deep Learning (DeLe) to identify patterns and clusters of patterns. Natural Language Processing (NLP), is the heart of modern Artificial intelligence (ArIn) input/output system. The capacity to comprehend natural language offers two crucial abilities [34]. The first is the capacity to understand unstructured material, such as 2.5 million peer-reviewed articles released annually, and the second is the capacity to communicate with a computer in plain language and have it understand our commands.

6.1.17 Policies and Topography

Two Artificial Intelligence (ArIn) methods to implement data breach prevention methods for network security are policies and topography. After the IT team establishes the policies, Artificial Intelligence (ArIn) can implement a variety of them. Therefore, Artificial Intelligence (ArIn) is useful in Cyber Security (CySe) in maintaining policies and effectively providing data protection through topography. It requires a lot of time and effort to decide on a set of workloads for staff. However, this feature makes it possible to offer workload sharing and effective security policies.

6.2 Weakness

6.2.1 Cyber Criminals

Hackers can employ Artificial intelligence (ArIn) security solutions as well. Additionally, Cyber security (CySe) teams operate in a far more transparent manner than cyber-criminals do. We are unlikely to gain from the experience of hackers, but they could be able to use our advancement and turn around our discoveries to make a more dangerous menace. To make their malware resistant to Artificial intelligence (ArIn) based security technologies, the attackers test and refine it. Hackers can launch more sophisticated assaults and target systems by learning from already existing Artificial intelligence (ArIn) tools.

6.2.2 Cyber Threats Keep Evolving

Integration of Artificial intelligence (ArIn) into Cyber Security (CySe) does not guarantee the complete safety from all kinds of threats. Even artificial intelligence (ArIn) systems will require consistent redesign, maintenance, and improvement because malware and viruses are constantly evolving.

6.2.3 Continuous Training

Artificial intelligence (ArIn) approach requires ongoing human interaction and instruction. This fusion strategy produces reliable results and collaborates nimbly with threat researchers.

6.2.4 Data Sets

The lack of dis-aggregated data is a pervasive problem in Cyber security (CySe) research, often justified by citing issues of confidentiality. Artificial Intelligence (ArIn) models are trained using learning data sets. Multiple data sets comprising malicious codes, malware codes, and abnormalities must be accessible to security teams [32]. Dealing with real-world Cyber Security (CySe) issues can be challenging due to the collection, administration, and processing of unquantified data, which may be structured, semi-structured, unstructured, or meta-data.

6.2.5 False Alarms

End users have difficulties due to numerous false alarms. False alarms have a negative impact on critical replies, which causes the entire network to go down. A technique known as fine-tuning is used to decrease false alerts while maintaining security.

6.2.6 Complacency

Artificial intelligence (ArIn) consistent cyber assault detection and prevention has allowed hackers to create more sophisticated threats and attacks. These attackers are highly motivated as more people have access to Artificial intelligence (ArIn) techniques, which lowers the cost of developing new technology. With such a small budget, it's conceivable for cyber-criminals to create increasingly intricate and sophisticated malware. There has been an increase in cybercrime due to human complacency. The concerns of the human aspect of complacency are not adequately addressed in Artificial intelligence (ArIn) based solutions to Cyber Security (CySe).

6.2.7 Less Availability

Contrary to conventional anti-virus software, artificial intelligence (ArIn) still necessitates a significant amount of labour and computational capacity. Instead of spending time and money developing a unique Artificial intelligence (ArIn) solution, you can just install a ready made piece of software. The good news, however, is that security neural networks are getting more and more affordable thanks to advances in artificial intelligence (ArIn), which even small firms can now afford.

6.2.8 Costly Resources

To create and operate artificial intelligence (ArIn) systems, investment of a significant amount of time and money is essential to acquire resources like computer power, memory, and data. A Large amount of data and

input samples are also, required for the smooth operation of Artificial Intelligence (ArIn) systems, but, this requires a lot of time and resources in terms of storage and processing power. Therefore, in order to implement Artificial Intelligence (ArIn) technology, expensive and smart resources are needed.

6.2.9 Neural Fuzzing

Fuzzing is a software testing technique that involves using a large amount of random input data to identify the system's vulnerabilities. Artificial intelligence is used in neural fuzzing to rapidly test numerous random inputs [9]. By gathering data using the strength of Neural Networks (NeNe), hackers can discover the flaws in a target system, but the same strategy can be used to enhance software, by producing code that is more difficult to breach [8].

6.2.10 Complex Assaults

Cyber Security now faces fresh issues as a result of rapid improvements in ICT. Modern cyber assaults and threats are so complicated and advanced that they cannot be furthered by using conventional techniques or strategies. New procedures and strategies are necessary to combat sophisticated cyber attacks with scalability, adaptability, and flexibility.

6.2.11 Network Centric Warfare

Cyber events become dangerous when Network Centric Warfare (NCW) is used, necessitating an urgent need for radical reforms in cyber protection. Due to human restrictions and limitations as well as intelligence of viruses and worms, Network Centric environment needs intelligent sensors to detect, assess, and react to cyber assaults in a timely manner.

6.2.12 Limitations

Artificial intelligence (ArIn) approaches for Cyber Security (CySe) has numerous advantages, but it is not the sole security solution. The defensive system might not work properly when a human opponent strikes the intelligent security with a clear by passing goal. While this does not exclude us from using Artificial intelligence (ArIn) approaches, we should be aware of their limits.

6.3 Opportunities

6.3.1 Speed and Database

In a very short amount of time, Artificial Intelligence (ArIn) will analyze gigabytes of data and immediately find suspicious code fragments. Artificial Intelligence (ArIn) will also be able to process, store, and learn from previously discovered threats.

6.3.2 Predictive Analytics

One of the skills that smart robots excel at is pattern recognition, which is a method for evaluating data, including text and images. Finding patterns in data, whether visual or textual, can be done using both supervised (training data) and unsupervised (no training data) methods. To predict potential developments, Artificial Intelligence (ArIn) solutions will analyze current threats, security news, and trends.

6.3.3 Unsupervised Learning

Unsupervised learning is a method that can be used to train artificial intelligence (ArIn). It will use un-labelled and unclassified data and special algorithms to enable Artificial Intelligence (ArIn) to learn independently as opposed to obtaining data from a human.

6.3.4 Knowledge Based Tools

Intelligent software will be able to defend against intelligent cyber weapons. By using the proper Artificial Intelligence (ArIn) approach and knowledge based technologies, comprehensive situational awareness and highly automated reaction to attacks the networks will also be possible.

6.3.5 Supervised Learning

The system will monitor the information input from which the learning algorithm will get its conclusions. A conclusion will be drawn using an expert system based on programmed inputs of subject matter experts. The usage of training data will result in advanced learning. Training a computer offers unique capabilities compared to expert systems, which rely on specialist-delivered precise solutions. Back propagation neural networks and logistic regression are two popular categories of learning algorithms.

6.3.6 Deep Learning

Deep learning (DeLe) is based on the concept that bigger neural networks improve as more data is used to train and scale them up.The ability of deep learning to detect malware and network breaches will be demonstrated.

6.3.7 Data Mining

Data Mining (DaMi) tools have a lot of potential for finding links between attacks. Data Mining (DaMi) would provide the search space more rational, scientific justifications [20]. Comprehensive Artificial Intelligence (ArIn) applications will outperform prediction and response by a greater margin in the identification of cyber threats.

6.3.8 Deep Reinforcement Learning

When faced with a new obstacle, it enables Artificial Intelligence (ArIn) to learn independently. In order to identify the best answer, deep neural networks and Q-Learning will use the concepts of state and action.

6.3.9 Automated Response

It involves combining preventative measures that don't involve direct human involvement and make use of a variety of systems, including firewalls, vulnerability scanners, security information and event management platforms, end user behaviour analytics, and endpoint protection solutions. This will result in very effective data protection practices and minimal human contact with information security. Additionally, it will lessen internal dangers and human errors. Additionally, this will improve procedures, manage threats, quickly coordinate the incident response, and detect weaknesses.

6.4 Threat

6.4.1 Perception and Decision

Four components make up artificial intelligence (ArIn) model: data observation, learning, decisions, and actions. It is called OLDA (Observe-Learn-Decide-Act) Loop. In a highly complex environment every component of OLDA (Observe-Learn-Decide-Act) Loop must interact with one another as they have mutual dependency. For instance, a wrong perception not corrected by previous learning can result in the wrong decision. We can say that perception is exposed to training assaults and decisions are vulnerable to classic cyber assaults.

6.4.2 Data

Artificial Intelligence (ArIn) approaches are also susceptible to adversarial assaults, which is one of the significant problems with data security. Data availability, data integrity, access control, network operation, and privacy are also under threat. Moreover, it should be understood that even the assaulters will use Artificial Intelligence (ArIn) to target and assault Artificial Intelligence (ArIn) based cyber defense systems for adversarial inputs, model theft and data poisoning.

6.4.3 Next Generation Viruses

To avoid detection, the next generation virus may devise an intelligent strategy for Kernel level operations or use root-kits. Additionally, the virus can recognize anti-virus software and create strategies for fighting its code [35]. The virus may continue its malicious operations by launching a new version after the anti-virus program identifies the old one.

6.4.4 Mimic Human Language

Viruses may imitate human speech and employ facial recognition software to fool people into sharing private information, granting access, or just engaging in cyber bullying [41].

6.4.5 New Threats

To prevent the system from misbehaving, a methodical program is required to confirm and corroborate the decisions, logic and risk analysis for similar and compatible elements of Artificial Intelligence (ArIn) and Machine Learning (MaLe). It's crucial to put new strategies into practice in order to meet system expectations, and respond to various assaults [42]. Therefore, the implementation of technology of Artificial Intelligence (ArIn) in the field of Cyber Security (CySe) may result in new risks, thus, putting the digital safety at risk.

6.4.6 Software Analysis

Artificial Intelligence (ArIn) techniques ignored and skipped the conventional software investigation and proposed a new assault bearing in the field of Artificial Intelligence (ArIn) algorithms [42]. A lot of accomplishments could be impacted by undiscovered dependent characteristics. Therefore, in-depth research is needed to create engineering concepts, new ideas, and practices before Artificial Intelligence (ArIn) may be used as a system element.

6.4.7 Limitations

The system would fail when a human adversary with a clear target for circumvention is aiming at intelligent defense. This does not demotivate us from using Artificial Intelligence (ArIn) approaches; rather, it simply means that we must be aware and careful of limitations [43]. Artificial Intelligence (ArIn) requires consistent training as well as human collaboration. It is necessary to conduct research on tool safety, threat modeling, environmental vulnerability, and human-machine collaboration.

6.4.8 Distant Infrastructure

Systems may now interact across continents and convey critical data around the globe. These transfers are not adequately protected and are more vulnerable to unauthorized access.

6.4.9 Detection and Reaction

Human teams cannot continuously pay attention to security concerns [30]. Due to this limitation and restriction, frequently, systems are not monitored. Instead of predicting dangers, most security specialists concentrate on dealing with them.

6.4.10 Dynamic Threats

Hackers use various tactics to hide their location, IP address, identity, and techniques. People are using various methods, including Virtual Private Networks (ViPrNe), Proxy Servers and Tor browsers, to evade detection and maintain anonymity [44]. In contrast, Cyber Security industry is much more open to research and transparent since hackers have easy access to business-generated data.

6.4.11 Integration of Technologies

The latest trend is integration of various Artificial Intelligence (ArIn) technologies. The field of Cyber Security (CySe) has made extensive use of computational intelligence techniques, but as the technology develops, there are some ethical and legal issues that arise, these challenges include questioning due process, privacy, legal precedent, the extent of technology taking human functions, and the extent of neural network replacing human judgement [46].

7. Research Gaps and Future Scope

7.1 Smart Sensors

The viruses and worms that infect and damage networks are also intelligent. This opens up the requirement of

developing smart sensors that can monitor and detect negative effects and eventually put a full stop to the extension and spread of viruses and worms.

7.2 Intelligent Cyber Defense

It is difficult to build intelligent cyber protection strategies in the current environment of malware with fast increasing intelligence and sophistication [6]. However, Distributed Denial of Service assault mitigation has highlighted that defense against large scale assaults can also be effective, if resources are employed using intelligent techniques [7]. It is well known that extensive research is being carried out in the field of Artificial Neural Networks (ArNeNe) but future research must also focus on other intelligent cyber defense technologies.

7.3 Decision Superiority

One of the challenges of Network Centric Warfare, is knowledge management. Guaranteed decision superiority can only be achieved by working on the development of decision making software that has modular and hierarchical knowledge architecture with the support of automated situation assessment [45].

7.4 Software Development

Smarter software is the trend in Cyber Security (CySe). As a threat response, software application development must be made more secure. Integrating Cyber Security (CySe) into the phases of software development will manage the risk involved in releasing new software that will immediately be under observation for loop holes and will be immediately attacked by hackers for vulnerabilities [46]. Hackers want to pierce the network by attacking the vulnerabilities and security professionals must protect the network using huge volume of log data, threat vectors, user behaviour, and analysis of structured threat intelligence with the help of Artificial Intelligence (ArIn) based Cyber Security (CySe) solutions.

7.5 Decision Agents.

Future work must enable groups of agents to make decisions. Unsupervised learning methods as well as new learning methods should be incorporated in implementation of Hybrid Model for intrusion detection [7].

8. Conclusion

This paper has carried out Strength, Weakness, Opportunities and Threat (SWOT) analysis of implementation of Artificial Technology (ArIn) techniques and methods in monitoring, analyzing, detecting and combating cyber assaults. It is important that the defender has the capability of fielding Artificial Intelligence (ArIn) technology in Cyber Security (CySe) with enhanced features. It has been proved time and again that Artificial Intelligence (ArIn) based Cyber Security (CySe) solutions are adaptable, flexible and robust, therefore better suited for improving security infrastructure, implementing the latest policies and better equipped to protect the system from a sophisticated, complex and large scale cyber threat. It is important to note that the amount and speed of data required to prevent cyber attacks cannot be managed by humans alone and requires significant automation. Superposition of Artificial Intelligence (ArIn) in Cyber Security (CySe) will not only add flexibility but also, incorporate learning capabilities.

A lot more research is required to achieve trustworthy geographically distributed systems that can manage distributed infrastructure, test the trained data for bias and robustness and feasibility of implementation at a small scale. Ups far outweigh the downs and hence, Artificial Intelligence (ArIn) must be implemented for speed, scalability, improving the accuracy of proactive protection and detection, enhancing the speed of investigation as well as implementing the automation in response.

References

[1] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3), 410.

[2] Shamiulla, A.M. (2019). Role of Artificial Intelligence in Cyber Security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628- 4630.

[3] Binny Naik, Ashir Mehta, Hiteshri Yagnik, Manan Shah.“ The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review’’, Complex & Intelligent Systems, 2021.

[4] Jin X, Liang J, Tong W, Lu L, Li Z (2017) Multi-agent trustbased intrusion detection scheme for wireless sensor networks. Comput Electr Eng 59:262–273

[5] Achbarou O, El Kiram MA, Bourkoukou O, Elbouanani S (2018) A new distributed intrusion detection system based on multiagent system for cloud environment. Int J Commun Netw Inf Secur 10(3):526

[6] Baig MM, Awais MM, El-Alfy ESM (2017) A multiclass cascade of artifcial neural network for network intrusion detection. J Intell Fuzzy Syst 32(4):2875–2883

[7] Roy SS, Mallik A, Gulati R, Obaidat MS, Krishna PV (2017) A deep learning based artifcial neural network approach for intrusion detection. International Conference on Mathematics and Computing. Springer, Singapore, pp 44–53

[8] Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.

[9] Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. In Artificial intelligence and evolutionary computations in engineering systems (pp. 351-363). Springer, Singapore.

[10] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 1-21.

[11] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 1-18.

[12] Aldhaheri S, Alghazzawi D, Cheng L, Alzahrani B, Al-Barakati A (2020) Deepdca: novel network-based detection of iot attacks using artifcial immune system. Appl Sci 10(6):1909

[13] Lyngdoh J, Hussain MI, Majaw S, Kalita HK (2018) An intrusion detection method using artifcial immune system approach. International conference on advanced informatics for computing research. Springer, Singapore, pp 379–387

[14] Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., ... & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. Current reviews in musculoskeletal medicine, 13(1), 69-76.

[15] Suhaimi H, Suliman SI, Musirin I, Harun AF, Mohamad R (2019) Network intrusion detection system by using genetic algorithm. Indonesian J Electr Eng Comput Sci 16(3):1593–1599

[16] Tao P, Sun Z, Sun Z (2018) An improved intrusion detection algorithm based on GA and SVM. IEEE Access 6:13624–13631

[17] AK. Ghosh, C. Michael, M. Schatz. A Real-Time Intrusion Detection System Based on Learning Program Behavior. Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, 2000, pp.93-109.

[18] Lidong Wang & Randy Jone. “Data Analytics for network intrusion detection". Journal of Cyber Security technology, Vol 4, 2020, Issue-2,Pgs 106-123.

[19] Naik N, Diao R, Shen Q (2018) Dynamic fuzzy rule interpolation and its application to intrusion detection. IEEE Trans Fuzzy Syst 26(4):1878–1892

[20] Gangavarapu T, Jaidhar CD, Chanduka B (2020) Applicability of machine learning in spam and phishing email fltering: review and approaches. Artif Intell Rev pp 1–63

[21] Jain AK, Gupta BB (2018) PHISH-SAFE: URL features-based phishing detection system using machine

learning. Cyber Security. Springer, Singapore, pp 467–474

[22] Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., ... & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. Current reviews in musculoskeletal medicine, 13(1), 69-76.

[23] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 1-21.

[24] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 1-18.

[25] Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. In Artificial intelligence and evolutionary computations in engineering systems (pp. 351-363). Springer, Singapore.

[26] Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In 2011 3rd International Conference on Cyber Conflict (pp. 1-11). IEEE.

[27] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1(1), 103-119.

[28] Thomson, V. (2016, April 21). Cyber Attacks could be predicted with Artificial Intelligence Help. PatternEX News

[29] D. A. Bitter, T. Elizondo, Watson. Application of Artificial Neural Networks and Related Techniques to Intrusion Detection. WCCI 2010 IEEE World Congress on Computational Intelligence. July, 18-23, 2010 - CCIB, Barcelona, Spain, 2010, pp. 949 – 954.