Artificial Intelligence in Cyber Security

Akash Hebbar
VI Sem, MCA
Department of MCA
RV College of Engineering,
Bengaluru

Dr S Anupama Kumar
Associate Professor
Department of MCA
RV College of Engineering,
Bengaluru

Abstract- In the field of Cyber Security there has been a development from the stage of Cyber Criminality to the stage of Cyber War over the last few years. Even though security devices are becoming modern and powerful, cyber-attack or cyber threats are increasing day by day. The main cause for this cyber-attack is our traditional threat detection methods to identify the threat or malware are falling apart. Cybercriminals are every day coming up with competent ways to bypass the computer security devices or programs and infect the network and computer systems with various kinds of malicious software's.

Artificial Intelligence changed each area it has been introduced. Credit Card Fraud Detection and Spam Filtering becomes possible due to the use of ML and AI algorithms these algorithms can study from historical fraud data and identify outliers and recognize them in future transactions. AI Algorithms able to works more efficient than humans when it comes to the data processing speed. Also, AI Algorithms can identify most difficult hidden fraud traces that a human cannot detect easily. AI can help to reduce number of false positives that may arise with use of out-of-date fraud identification methods. Artificial Intelligence methods has discovered that this is similarly efficient for all stages of the Cyber Security.

Keywords-Intrusion Detection System, Artificial Intelligence, Distributed Denial of Service

I. Introduction

A successful cyber-attack can have overwhelming consequences for an individual or business. Digital presence includes massive amounts of personal and financial data which cannot afford to lose. Attacks have the potential to substantially damage the reputation of a company or take it down entirely, and of course, many attacks begin with the weakest loophole in the chain – the human staffs and their devices. Artificial Intelligence (AI) cybersecurity, with the help of machine learning, is become an efficient tool in the upcoming future [2]. As compare to other businesses, human interaction has been important and irreplaceable in cyber security. While cybersecurity presently depends mainly on human input, and gradually seeing technology become better and better at specific tasks than pervious.

Human fault is important part of cyber-security weaknesses. For example, the efficient system configuration can be extremely tough to achieve, even with engaging huge number of IT teams in setup process. In the development of continuous innovation, computer security has advanced more layered than ever. Security Alert devices could help teams find and issues that identified in network systems and they can fix issue as soon as [2].

In addition, the privacy violations incidences are also addressed. As technologies are updating day by day we get, the additional ways to break cyber protection. These days, there's a huge raise in cybersecurity challenges. This paper intends to give an overview use of several applications of AI practices as well as examines how AI systems could be protected organization from daily cyber-attacks. And also explain advantage and disadvantage of integrating AI in Cybersecurity Applications

The paper is divided into six sections, the introduction, literature survey, artificial intelligence in cyber security, present-day cybersecurity, and its future with ai, algorithms used in artificial intelligence enabled applications and limitations of artificial intelligence

II. Literature survey

Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu. Survey on The Applications of Artificial Intelligence in Cyber Security [1]. This paper gives an idea of how Artificial Intelligence can be integrated in cyber security field. And Some AI best practices used in cyber security field such as DL or Deep neural network.

Shruthi Kohli. Developing Cyber Security Asset Management framework [2]. This paper explains how Cyber Threat put Emerging technologies and business in various risk such data breach, unauthorized access, malwares. Also explains how new developments in defensive security policies of specialists fail at some point.

Roumen Trifonov, Ognyan Nakov,Valeri Mladenov. Artificial Intelligence in Cyber Threats Intelligence [3]. This paper gives some detailed explanation of results obtained from Multi-Agent System Project using Recurrent Neural Networks and explains how these how these Agent System can be efficiently used for security devices.

Arthur Samuel [4], a pioneer in artificial intelligence, describes ML as a set of diverse methods and technologies that provides ability to computer it can learn without being explicitly programmed." Example supervised machine learning for anti-malware applications and also, he explains about Decision tree classifier method used in predictive model, and it takes the set of decision trees (random forest or gradient boosted trees) [5]. Every non-leaf node of decision tree covers some question about features of a file or data, while the leaf nodes cover final decision of the tree on data object. And by using this technique how computer system can efficiently classify normal and abnormal transactions.

Soorena Merat, Wahab Almuhtadiin. Artificial intelligence application for improving cyber-security acquirement [5]. In this paper author explains how improvement of ML algorithms changed threat detection accuracy and also explains various types of computer processes can be mapped in multitasking situation. A software mapping and modelling system called SHOWAN is implemented to study and classify the cyber awareness of a computer process against multiple concurrent threads.

Bhavani Thuraisingham. The Role of Artificial Intelligence and Cyber Security for Social Media. This paper explains the role of both AI and Cyber Security methods for social media systems and how effectively these methods can be used to protect social media platforms. And also explains vulnerability identification in social media platforms

AI plays very important role to offload work from human cybersecurity engineers, to handle the depth and detail that humans cannot identify fast enough or precisely enough. Improvement in machine learning techniques means that AI applications can also automatically adapt to improvements in threats identification. AI can helps speed up threat detection process, rapidly cross-referencing different alerts and sources of security data [6]. Human cyber security specialists will still priorities of the incidents to be handled but can be additionally helped by AI systems that automatically recommend plans for improving responses.

III. Artificial intelligence in cyber security

AI can efficiently analyse user behaviours, assume a pattern, and recognize all sorts of anomalies or loopholes in the network. With such data, it's much easier to recognize cyber weaknesses rapidly. And responsibilities which are now reliant on human skill will be susceptible to malicious cyber programs imitating legitimate AI-based algorithms. The following are some of the important advantages of using AI [7].

- **Threat response time**

Threat identification and response generation time is the very important system of measurement for a cybersecurity teams' efficiency. Performance efficiency of security systems are measured based on how quickly system able to identify threat and give response or alert back to users.

AI – Enabled systems can take data from attack and instantly make cluster and prepare for analysis. And then apply various ML and AI algorithms on data. And generate report by using this report makes security specialist decision-making process easier

- **Human efficiency with repeated activities**

Human threat detection effectiveness is other point for cybersecurity business. No manual threat detection process can perfectly repeated multiple times, particularly in a changing environment. The separate setup of multiple endpoint devices for organization is most time-consuming job. Even after initial device setup, IT teams need to check or revisiting the same devices later for identifying and rectifying misconfigurations or old configurations that cannot be patched or fixed in remote bug fix updates. By using AI security teams can solve these problems easily

- **Vulnerability management**

Companies are finding difficulty to prioritize and manage the massive volume of zero-day vulnerabilities they detect on a day-to-day basis. Old-style vulnerability management approaches tend to wait for attacker to exploit high-risk vulnerabilities before deactivating them.

While traditional vulnerability databases are difficult to manage and comprise known vulnerabilities, different Artificial Intelligence and machine learning methods like User and Event Behavioural Analytics (UEBA) can detect baseline of user accounts and endpoint and servers and identify malicious behaviour that might signal a zero-day attack. This can help organizations to protect themselves even before vulnerabilities are officially reported and bug fix updates are released.

IV. Present-day cybersecurity and its future with ai

Today, business focus to their system security. They are aware of the huge impact of every small and large-scale cyber-attack. To secure this organization, organizations use multiple types of defence. This multi layered security devices usually begins with the top suitable firewall capable of governing and filtering out the incoming network traffic. After this layer, the second line of defence consists of antivirus software. These Antivirus applications scan through the system to find and detect suspicions codes and malicious files. Simply way to defense against cyber-attack, business frequently take data backups as a part of a disaster recovery policy [7].

- Setting firewall policies, maintaining backups, and other tasks require a expert, but AI will change the traditional method.

- Administrations will be able to monitor and retort to security events by using advanced tools.
- The next-generation firewalls will have in-built machine learning technology that could detect a outline in network packets and block them automatically if flagged as a threat.
- Predictably, the natural language capabilities of AI will be used to understand the origination of cyber-attacks.

V. Algorithms used in artificial intelligence enabled applications

Artificial Intelligence has grown to have a significant impact on the world. With large volumes of data being produced by different applications, machine learning systems able learn from the test data and perform intelligent tasks. AI-driven security from three different perspectives, based on the sources of data on which analytics is being applied, based on machine learning methods being used or based on intended results to be achieved.

Machine learning is a part of AI focused on developing applications that acquire knowledge from data and improves their prediction accuracy over time without manually coded to do so. Machine learning deals with applications that learn from past experience and progress their decision-making or predictive ability and accuracy over time.

Classification is the method of separating the dependent variable into sub class and then predict a class for a given input data. It is part of Supervised Machine Learning.

Classification Algorithm’s widely used in AI applications because this algorithm can easily classify normal and abnormal pattern in data based on past experience. For example, Random Forest and Decision Tree algorithm can be used in Network Intrusion Detection and Spam Filtering Application because algorithms can easily classify normal and abnormal data and it provide very good accuracy rate.

A. Random Forest

Random Forest Machine Learning Algorithm based on Decision Tree. It is a combination of multiple Decision Tree that work together to make prediction. These tree work on random subset of data. [6].

Accuracy – Defined as the ratio of correctly

classified samples to total number of samples.

$$\text{Accuracy} = \frac{\text{Samples correctly classified in test data}}{\text{Number of samples in test data}} \qquad (1)$$

B. K-means Algorithms

K-means algorithms is un-supervised machine learning method, works based on distance measurement of object and then classify the objects into clusters. It is one of the popular machine learning algorithms [13]. K-means algorithms works by if finds similarity in dataset and group the data, Measure distance or similarity plays an important role in collecting observations into homogeneous groups. where the number of groups is represented by the variable k [10].

$$\underset{S}{\arg\min} \sum_{i=1}^{k} \left(\sum_{x_j \in S_i} \|x_j - \mu_i\|^2 \right) \qquad (2)$$

C. Decision Tree

Decision Tree Approach classifies the data using series of rules and this is tree like model which makes it interpretable. These trees can automatically exclude duplicate features.

Decision tree learning process consist different phases like features selection, tree generation and tree pruning. In Training phase this model selects the best suitable features individually and then it generates child nodes from the root node [10].

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (fi - yi)^2 \qquad (3)$$

Where N is the number of data points, fi is the value returned by the model and yi s the actual value for datapoint i.

This formula calculates the distance of each node from the predicted actual value, helping to decide which branch is the better decision for your forest. Here, yi is the value of the data point you are testing at a certain node and fi is the value returned by the decision tree [9].

VI. Artificial intelligence (ai) techniques for cyber security

Artificial Intelligence practices are the key to Interference detection and make it possible to respond even to anonymous threats before spreading itself. Artificial Intelligence techniques are broadly classified into three groups such as expert system, Intelligent agents, and Natural Language Processing

- **Expert Systems:**

Expert System is a computer device that duplicates the decision-making power of a person. This is a suitable example of Knowledge based system. These knowledge-based devices are made of two sub-systems: such as Knowledge Base and the Inference Engine. The knowledge base denotes the illustrations and assertions in the real world. Inference Engine an automatic reasoning system. It estimates the present state of the knowledge base and applies the rules applicable to that, then asserts new knowledge into it.

- **Intelligent Agents:**

Intelligent Agent (IA) is a software that exists in an environment, which is not controlled externally, responds to fluctuations in its environment, persistently pursues goals, has multiple ways of achieving goals, recovers from failure and interacts with other agents. Mainly IA devices is created to avoid Distributed Denial of Service attacks. A best way to use agents against distributed cyber-attacks is by construction of best artificial Digital policy for organisation

- **Natural Language Processing:**

Natural Language Processing, it is a deep learning technique, It can help to easily identify and deal with spam and other different types of social engineering. NLP learns normal flow of communication and it identify language patterns and uses numerous statistical models to identify and block or filter spam. Deep learning ANNs are showing best results in examining HTTPS network traffic to identify for suspicious activities. This is also useful to deal with different cyber threats such as SQL injections and Distributed Denial of Service attacks.

VII. Drawbacks and limitations of using ai for cyber security

The benefits mentioned above are the potential of AI in helping cyber security, but there are also restrictions which are stopping AI from becoming a mainstream tool used in the Cyber Security field. In order to build and preserve AI system, companies would need a huge number of resources including memory, data, and computing power. Additionally, because AI devices are trained through learning data sets, cyber security firms need to get their hands on many different data sets of malware codes, non-malicious codes, and anomalies. Obtaining these precise data sets requires really long time and resources so this will lead company to lots of expenses so some companies cannot afford.

VIII. Conclusion

Artificial Intelligence has emerged as essential technology for enhancing the work of human information security teams. Since humans can no longer scale to protect the dynamic enterprise attack surface, Artificial Intelligence provides detailed analysis and alert so threat identification that can be easier for cybersecurity professionals to reduce number breach risk and improve overall security. Main advantage of AI it can identify and prioritize risk according to priority cybersecurity professionals handle risks. Artificial Intelligence allows cybersecurity group to create a powerful human-machine partnership that push the limit of knowledge, enrich lives, and drive cybersecurity in a way that seems greater than the sum of its parts.

IX. References

[1]. Shidawa Baba Atiku, Achi Unimke Aaron, " Survey on The Applications of Artificial Intelligence in Cyber Security, ITU, and WCIT", 2019 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 119-134, 2019

[2]. Shruthi Kohli. “Developing Cyber Security Asset Management framework., (IJARAI) International Journal of Advanced Research in Artificial Intelligence”, vol. 2, no. 4, 2018

[3]. O. Oriola, A. Adeyemo and A. Robert, "Distributed Intrusion Detection System Using P2P Agent Mining Scheme", African Journal of Computing & ICT, vol. 5, no. 2, 2020

[4]. E. Menahem, A. Shabtai, L. Rokach, and Y. Elovici, ‘‘Improving malware detection by applying multi-inducer ensemble,’’ Comput. Statist. Data Anal., vol. 53, no. 4, pp. 1483–1494, Feb. 2013.

[5]. Ionita and L. Ionita, "An agent-based approach for building an intrusion detection system",RoEduNet International Conference 12th Edition: Networking in Education and Research, pp. 1-6, 26-28, 2020

[6] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, ‘‘A distributed anomaly detection system for in-vehicle network using HTM,’’ IEEE Access, vol. 6, pp. 9091–9098, 2018, doi: 10.1109/ ACCESS.2018.2799210.

[7]. J.Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications, vol. 8, no. 1, pp. 247-256, 2014