International Journal of Computer Applications Technology and Research
Volume 13–Issue 01, 07 - 08, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1301.1002

Reinventing Cyber Security with AI

Dr.A.Jeyalakshmi
Associate Professor
Sri Ramakrishna College of Arts and Science
Coimbatore, Tamil Nadu, India

Abstract: In the digital age, data is the new gold, and a valuable asset, it needs to be safeguarded. Cyber security has always been a critical concern for individuals and businesses alike, but as technology advances, so do the threats that seek to compromise the data. In response to this escalating issue, artificial intelligence (AI) is stepping up to the plate, offering innovative solutions that are reinventing the way to protect the data. This paper provides a concise overview of AI implementations of various cyber security using artificial technologies and evaluates the prospects for expanding the cyber security capabilities by enhancing the defense mechanism

Keywords: Artificial Intelligence, Intelligent Agents, Neural networks, Smart Cyber Security methods.

1. INTRODUCTION

Cyber security is important because it encompasses everything that relates to protecting our data from cyber attackers who want to steal this information and use it to cause harm[1][2][3]. This can be sensitive data, governmental and industry information, personal information, personally identifiable information (PII), intellectual property, and protected health information (PHI). Therefore, they are obviously vulnerable to cyber attacks. A cyber attack is an attack launched from one or more computers against cyber attacks is either to disable the target computer, or take the services offline, or get access to the target computer's data[4]. In response to the issues, artificial intelligence tools are commonly implemented to deal with cyber threats. Artificial intelligence (AI) has helped more organizations to improve the security posture effectively and reduce the breach risks. Machine learning and artificial intelligence are the essential tools in technology for information security as it helps companies and individuals to check and analyze the threats posed to the organization [5].

2. LITERATURE REVIEW

Many more research works have been reported for cyber security threats, predicting the cyber threats with machine learning and deep learning algorithms in AI.Vipin Kumar [1] used a simple k-means clustering approach on NSL-KDD dataset to perceive the accuracy for intrusion detection. K-means, an unsupervised algorithm, is used for classification and defines an unlabeled class to which the clustering is performed. Rahman Ali, et al.,[5] reported A systematic literature review of existing classification algorithms, applied to the area of detection of cyber security attacks is presented and it is concluded that Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT) and Artificial Neural Network (ANN) are the most frequently used classifiers. Jie Chen. et al.,[6] suggested that AI algorithms are mainly applied in cyber security to predict the threats using Machine learning and deep learning.

3. RESEARCH METHODOLOGY

3.1 Cyber Security Challenge

Cyber security is essential for protecting digital assets, including sensitive personal and financial information, intellectual property, and critical infrastructure. The most difficult challenge to cyber security is adapting to a remote workforce. With more and more companies around the world turning to remote work, there are new risks in cyber security that have emerged. Companies must now invest in solutions that protect their systems from attacks outside their networks. The most common cyber threats are phishing, malware, and ransom ware. Phishing is a type of online fraud that involves attackers sending fake emails or websites that look legitimate in order to trick victims into entering personal or financial information. Due to most of the organizations gets challenges in financial loss, reputational damage, and even physical harm.

3.2 AI based Cyber Security Process

3.2.1 Threat Detection

AI algorithms have the capability to analyze huge volumes of data in real time objects, identify patterns, monitor network traffic ,user behaviour, and system logs that could signal a potential security breach.

3.2.2 Predictive Analysis

Predictive analysis is a statistical method which is used to gather data from historic data.AI algorithms to predict anomalies, identify patterns and create forecasts. Predict future threats and attacks and create safety borders for them.

3.2.3 Zero Trust Architecture:

The principle of ZTA is "Never Trust, Always Verify". AI assists in continuously monitoring and analyzing user behaviour, devices, and network traffic to ensure trustworthiness. If an unusual or suspicious activity is detected, AI can swiftly trigger security measures to restrict access until trust is re-established.

3.2.4 BlockChain Technology

Recently, [7] crypto currencies have popularly increased in the market. These are processed based on block chain technology and provide an innovative technical solution for secure transactions and saving the money. Block chain can be used to enable medical records and help in security management by identifying criminal identity loopholes in the system. [7] With block chain technology, verification keys wouldn't be required anymore. If someone tries to hack the

data, the system analyzes the whole mass of data chains. Even if one data node is left uninterrupted by the hacker, the entire system can be restored successfully.

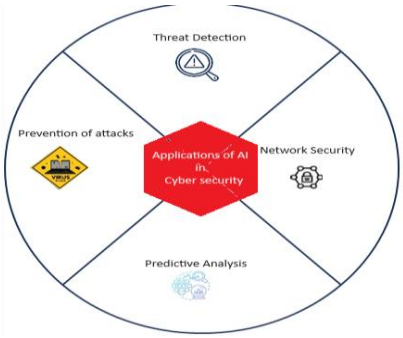

Fig 1 : Applications of Artificial Intelligence in Cyber Security

4. AI BASED CYBER SECURITY CHALLENGES:

AI in cyber security is a double edged sword which enhances and secures threats in all direction. Though, some challenges also exist. The lack of resources to build and maintain AI Systems in cyber security. Vulnerability of AI systems to attacks, infiltration, and manipulation by adversaries also, Inconsistency and privacy concerns around data laws, policies, and regulations.

5. CONCLUSION:

Artificial Intelligence is a fast growing technology in the current era for improving digital security.AI gives a needed analysis and threat identification that can be used by security professionals to minimize breach risk and enhance security posture. Also, As many harmful threats can be detected before any damage, security experts will have more response time to fight against these malicious attacks. Though AI is a valuable asset in cyber security, its limitations-such as data dependencies, false alarms and lack of transparency-should be carefully considered when integrating AI into security strategies.

6. REFERENCES

1. Vipin Kumar, Himadri Chauhan, Dheeraj Panwar,"K-Means Clustering Approach to Analyze NSL-KDD Intrusion Detection Dataset",International Journal of Soft computing and engineering,2013,3,4, 2013, ISSN: 2231-2307.
2. Torres, J.M., Comesaña, C.I., García-Nieto, P.J. Machine learning techniques applied to cybersecurity.International journal of machine learning and cybernetics. 2019, 1–14.
3. Hashemi, H., Azmoodeh, A., Hamzeh, A., Hashemi, S. Graph embedding as a new approach for unknown malware detection. Journal of computer virology and hacking techniques, 2017, 13, 153–166.
4. Ab Razak, M.F., Anuar, N.B., Othman, F., Firdaus, A., Afifi, F., Salleh, R. Bio-inspired for features optimization and malware detection. Arabian journal of science and engineering,. 2018, 43, 6963–6979.
5. Rahman Ali, Asmat Ali, Fark Hund Iqbal, Asad Masood Khattak and Saiqa Aleem," A Systematic Review of Artificial Intelligence and Machine Learning Techniques for Cyber Security", International conference on big data and security, August 2020,584-593.
6. Jie Chen,Dandan Wu,Ruiyun Xie, "Artificial intelligence algorithms for cyberspace security applications: a technological and status review", Frontiers of Information Technology and Electronic Engineering, August 2023,24,1117-1142.
7. Gaurav Belani, **"**The Use of Artificial Intelligence in Cybersecurity: A Review", IEEE Computer society,2021.