IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI BASED COMPUTER NETWORK SECURITY

[1]Shyamalendu Paul, [2]Amitava Podder

[1]Assistant Professor, [2]Assistant Professor
Department of Computer Science & Engineering
Brainware University, Barasat, India

Abstract: Computer networks are integral to business, communication and personal activities in today's society. However, the rapid expansion of computer networking capabilities has also increased cyber-attacks and security threats. Artificial intelligence (AI) has been hailed as a promising technology for improving network security. AI-based computer network security systems have the potential to automatically detect, respond to and prevent network security threats. This research paper explores the concept of AI-based computer network security systems, their benefits and limitations, and the potential for future developments.

Index Terms **- Artificial intelligence (AI), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Natural Language Processing (NLP).**

I. Introduction

Computer networks are a critical part of our modern society, and they play a significant role in almost all aspects of our lives, including business, communication and personal activities. However, as the use of computer networks continues to increase, so do cybersecurity threats that can cause significant damage to individuals and organizations alike. Data security has become a major concern for organizations in today's digital age. Cyber-attacks have increased exponentially in the recent past, and they have become more sophisticated and complex. [1] With the increase in the frequency and complexity of such attacks, traditional security measures are no longer sufficient to protect computer networks. Therefore, there is a need for advanced security systems that can mitigate the risks associated with these attacks. As such, a new approach to network security is needed, with artificial intelligence (AI) playing an increasingly essential role in developing more robust and efficient security measures. Artificial intelligence (AI) can be used to develop computer network security systems that can detect and prevent malicious activities. [5] [6]

II. IMPORTANCE OF NETWORK SECURITY

Network security has become a critical concern for organizations with the increasing dependence on computer networks to store and process sensitive information. [2] Any data breach could result in a significant loss of financial and reputation damages. Therefore, it is essential to secure the computer network to protect against unauthorized access, data theft, and other malicious activities. [13]

III. Current Network Security Approaches

Currently, organizations use a range of different security measures to protect their computer networks. These include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and data encryption systems. [11] However, these methods are not foolproof, and some attacks still find their way through these defenses. Furthermore, these systems often require significant human intervention to detect and mitigate these attacks. [12]

Here are some of the current network security approaches:

3.1 Firewalls: A key element of network security is the firewall. Based on pre-established security criteria, they keep track of and regulate both incoming and outgoing network traffic. Firewalls are network packet inspection and security policy enforcement tools that can be either hardware or software-based.

3.2 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): To identify and stop unauthorised network access and attacks, IDS and IPS technologies are utilised. While IPS systems go one step further by actively thwarting or stopping the threats they have identified, IDS systems monitor network traffic and create alerts when suspicious activity is identified.

3.3 Virtual Private Networks (VPNs): By encrypting the data exchanged between the user's device and the network, VPNs establish secure connections across open networks. With the use of VPNs, data is protected from interception and tampering by maintaining confidentiality, integrity, and authenticity.

3.4 Secure Sockets Layer/Transport Layer Security (SSL/TLS): Secure internet communication is made possible by the cryptographic technologies SSL and TLS, which succeeded it. They create secure connections between web servers and clients, guaranteeing the confidentiality and integrity of any data transferred.

3.5 Network Access Control (NAC): Access to a network can be managed and controlled with the use of NAC solutions. They often entail confirming users' and their devices' identities, examining compliance with security policies, and, based on the findings, issuing the proper network access credentials.

3.6. Secure DNS: One of the most important parts of the internet's architecture is DNS (Domain Name System). Digital signatures are added to DNS data by secure DNS protocols like DNSSEC (Domain Name System Security Extensions), which ensure the authenticity and integrity of the data. By doing this, DNS hijacking and other DNS-related threats are deterred.

3.7 Security Information and Event Management (SIEM): SIEM systems gather and examine security-related data from a variety of network sources, including servers, firewalls, and IDS/IPS. By correlating and analysing log data and producing warnings for questionable actions, they offer real-time monitoring, threat detection, and incident response capabilities.

3.8 Application-level Gateways (ALGs): In accordance with security guidelines, ALGs monitor network traffic at the application layer and permit or deny particular protocols or services. They can offer extra security features including content filtering, protocol validation, and deep packet inspection.

3.9 Network Segmentation: A network is segmented when it is broken up into several smaller subnetworks, also referred to as segments or VLANs (Virtual Local Area Networks). This lessens the possible impact of a security compromise by preventing unauthorised access and isolating key systems.

3.10 Next-Generation Firewalls (NGFW): With the addition of additional security features like application awareness, intrusion prevention, deep packet inspection, and sophisticated threat intelligence, NGFWs combine classic firewall functions. They give network traffic, including application-level controls, more visibility and management.

IV. Definition of AI-Based Computer Network Security System

An AI-based computer network security system is a security system that makes use of AI techniques to detect, respond to, and prevent network security threats. This system is dedicated to automating the process of monitoring and responding to potential threats, thereby freeing up security personnel to focus on more strategic tasks.

V. BENEFITS OF AI-BASED COMPUTER NETWORK SECURITY SYSTEM

AI can help to improve the effectiveness of computer network security systems by providing more advanced threat detection, analysis, and response capabilities. [3] AI tools can help to identify various types of cyber threats, including zero-day exploits, targeted attacks, and malware. It can also detect unusual network activity that might signal a possible attack. [4] AI-assisted systems can automatically respond to the detected incidents and reduce the time required to detect and mitigate cyber threats.

The benefits of AI-based computer network security systems can be grouped into accuracy, speed, and adaptability. [7] [8]

5.1 Accuracy: AI-based systems can be trained to recognize and classify a vast number of potential security threats, often far more accurately than humans. They can also continue to learn and evolve over time, leading to more accurate and effective responses to potential threats. By automating the threat identification process, the risk of human error can be minimized, and the security system becomes more reliable.

5.2 Speed: AI-based computer network security systems can analyze vast amounts of data and detect potential threats in real-time, significantly reducing the response time to an attack. They can also respond to threats more quickly than a human analyst, thereby minimizing the damage that an attack can cause.

5.3 Adaptability: AI-based computer network security systems can adapt to new threats quickly. They can self-learn new threat characteristics, thereby improving their ability to detect and prevent attacks in the future.

VI. TECHNOLOGIES USED IN AI-BASED NETWORK SECURITY

There are several technologies that can be used in an AI-based network security system. [14] These include machine learning algorithms, neural networks, natural language processing (NLP), and data analytics.

6.1 Machine Learning:

Machine learning algorithms are able to analyse enormous volumes of data and spot trends that point to harmful behaviour. It can also detect unfamiliar activity that is inconsistent with a system's normal behavior. Hence, it can help to accurately identify and mitigate cyber threats. [9] [15]

6.2 Neural Networks:

Neural networks can learn from previously analyzed data to detect and prevent cyber-attacks. They can help to build a list of known attacks, and their features can help to identify new attacks. [10]

6.3 Natural Language Processing:

NLP can help in identifying unusual patterns in network traffic. It can help make the system more intelligent, allowing it to detect potential threats by analyzing the language or content of network traffic.

6.4 Data Analytics:

Data analytics can be used to identify patterns in network traffic that could indicate an attack. It can also help to analyze the large datasets generated by network security systems to improve the system's performance.

VII. LIMITATIONS OF AI-BASED COMPUTER NETWORK SECURITY SYSTEM

Despite the significant benefits of AI-based computer network security systems, there are also some limitations. One of the most significant challenges is the potential for the system to generate false positives, which can lead to a significant amount of irrelevant alerts and wasted resources. [16] [17] Additionally, an AI-based system may be limited by its training data since it can only detect threats that have been previously identified. Therefore, it is essential to ensure that the training data used in developing AI-based security systems are comprehensive and well-structured.

Here are a few important considerations:

7.1 Limited Training Data: For AI systems to learn and develop reliable predictions, a large amount of high-quality training data is necessary. Getting huge, diversified datasets that cover all potential threat scenarios can be difficult in the realm of network security. The AI system may have trouble effectively identifying new and emerging risks if the training data is inaccurate or biassed.

7.2 Adversarial Attacks: Adversarial assaults entail faking input data on purpose to trick AI systems. Attackers can take advantage of holes in AI models by inserting harmful material that has been specifically designed to go beyond security precautions. If the right countermeasures are not in place, adversarial assaults could compromise the effectiveness of AI-based network security solutions.

7.3 Lack of Explainability: Many AI systems, including deep learning models, are referred to as "black boxes" because they are opaque in how they make decisions. It may be difficult for network administrators and security professionals to comprehend the rationale behind specific judgements or predictions due to this lack of explainability. Trust issues, troubleshooting issues, and performance tuning issues may result as a result.

7.4 False Positives and False Negatives: AI-based network security solutions could produce false positives or false negatives, misclassifying harmless activity as harmful or failing to identify real threats. False positives can cause a security team's workload to increase and unnecessary warnings to be sent out, which could cause them to become alert fatigued and overlook real threats. Networks may become exposed to attacks as a result of false negatives, which could result in breaches.

7.5 Rapidly Evolving Threat Landscape: Threats to network security are constantly changing and getting more advanced. For AI models to quickly detect and counteract new sorts of threats, they must be flexible. However, the process of training and upgrading AI models can take a while and may lag behind the quick pace of new threats. Networks may become exposed to recently developed attack methods as a result of this time gap.

7.6 Dependence on Historical Data: To make predictions, AI models significantly rely on past data. Historical data may, however, become less useful or out of date if the danger landscape drastically changes. The ability of AI-based network security solutions to detect and respond to innovative and zero-day attacks may suffer as a result.

7.7 Ethical and Privacy Concerns: Network security AI technologies may cause ethical and privacy issues. Process sensitive user data as part of network traffic monitoring and analysis to spot potential risks. It can be difficult to strike a balance between respecting user privacy rights and effective security measures.

VIII. FUTURE DEVELOPMENT OF AI-BASED COMPUTER NETWORK SECURITY SYSTEM

The future development of AI-based computer network security systems is primarily in deep learning, a subset of machine learning that involves training neural networks with large datasets. [19] By using deep learning, AI-based security systems can learn and detect new kinds of threats, even without prior knowledge, which will significantly improve their effectiveness in identifying and responding to cyber-attacks. Additionally, the integration of blockchain technology into AI-based computer network security systems will enhance data privacy and integrity, thereby creating more secure network systems. [18] [20]

IX. CONCLUSION

As the cybersecurity threat landscape continues to evolve, so must network security measures. AI-based computer network security systems offer many advantages over traditional security measures such as improved accuracy, speed, and adaptability. Despite some potential limitations, AI-based security systems are becoming increasingly important in the development of a more robust and efficient network security system. AI has the potential to revolutionize the field of network security. AI-based computer network security systems can help to identify and mitigate cyber threats more efficiently than traditional security systems. They can provide advanced threat detection, analysis, and response capabilities, making them essential to secure computer networks. However, developing these systems requires overcoming several challenges related to data quality, false positives, generalization, and causality, making it necessary to develop new methods and approaches. The future of the development of AI-based security systems lies in deep learning and the integration of blockchain technology.

REFERENCES

[1] Josh Fruhlinger, “What is cyber attack?,”. CSO, February 2020. https://www.csoonline.com/article/3237324/whatis-a-cyber-attack-recent-examples-showdisturbing-trends.html.

[2] Cavelty, Myriam Dunn, “ The Routledge Handbook of New Security Studies,”. 154-162, 2018.

[3] Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. SIN’09 - Proceedings of the 2nd International Conference on Security of Information and Networks, 229–234. https://doi.org/10.1145/1626195.1626252.

[4] Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3973 LNCS, 255–260. https://doi.org/10.1007/11760191_37.

[5] John McCarthy,” Artificial Intelligence logic and formalizing common sense,” Stanford University, CA, USA 1990

[6] Lidestri, N., Maher, Stephen J., & Zunic, Nev.,” The Impact of Artificial Intelligence in Cybersecurity,”. ProQuest Dissertations and Theses, 2018.

[7] Russell Stuart J., Norvig, Peter (2003), “ Artificial Intelligence: A Modern Approach, “. (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13- 790395-2.

[8] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a multiagent environment for military decision support tools with semantic services. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6070 LNAI(PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7_19.

[9] Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS’07). 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10]. Pravin Kshirsagar and Sudhir Akojwar (2017), “Classification of ECG-signals using Artificial Neural Networks”, Researchgate.net

[11]. Amitava Podder, Satyaki Kumar Biswas. "Energy-Efficient Passive Optical Network (PON) Planning with Wavelength Allocation Scheme based on User Behaviors and Bit Error Rate (BER) Performance Evaluation", *International Journal of Engineering Science Invention (IJESI)* ISSN (Online): 2319-6734, ISSN (Print): 2319-6726 www.ijesi.org ||Volume 10 Issue 2 Series I || February 2021 || PP 01-11 || Journal DOI-10.35629/6734.

[12]. Alterazi HA, Kshirsagar PR, Manoharan H, Selvarajan S, Alhebaishi N, Srivastava G, Lin JC-W. Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. Sensors. 2022; 22(16):6117. https://doi.org/10.3390/s22166117.

[13] S. B. Atiku, A. U. Aaron, G. K. Job, F. Shittu, and I. Z. Yakubu, "Survey On The Applications Of Artificial Intelligence In Cyber Security," International Journal of Scientistic and Technology Research, vol. 9, pp. 165-170, 2020.

[14] Benoit Morel, “Artificial Intelligence a Key to the Future of Cybersecurity,”. In Proceeding of Conference AISec’11, October 2011, Chicago, Illinois, USA.

[15] Chowdhury, M., Rahman, A., Islam, R., “Malware analysis and detection using data mining and machine learning classification,”. In Proceedings of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Ningbo, China, 16–18 June 2017; pp. 266-274.

[16] Biswas, S.K., Podder, A. (2022). "*Path Minimization Planning and Cost Estimation of Passive Optical Network Using Algorithm for Sub-optimal Deployment of Optical Fiber Cable".* In: Mitra, M., Nasipuri, M., Kanjilal, M.R. (eds) Computational Advancement in Communication, Circuits and Systems. Lecture Notes in Electrical Engineering, vol 786. Springer, Singapore. https://doi.org/10.1007/978-981-16-4035-3_7.

[17] H. Hashemi, A. Azmoodeh, A. Hamzeh, S. Hashemi, “Graph embedding as a new approach for unknown malware detection,”. J. Comput. Virol. Hacking Tech. 2017, 13, 153-166.

[18] Y. Ye, L. Chen, S. Hou, W. Hardy, X. Li, “DeepAM: A heterogenous deep learning framework for intelligent malware detection,”. Knowledge Information System. 2018, 54, 265-285.

[19] N. McLaughlin, J. Martinez del Rincon, B. Kang, S. Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupe, “Deep android malware detection,”. In Proc of the Seventh ACM on Conference on Data and application Security and Privacy, Scottsdale, AZ, USA, 22-24 March 2017, pp.301-308.

[20]I. A. Mohammed, "Artificial Intelligence For Cybersecurity: A Systematic Mapping of Literature," International Journal of Innovations In Engineering Research and Technology [IJIERT], vol. 7, 2020.