Journal of Informatics Education and Research
ISSN: 1526-4726
https://doi.org/10.52783/jier.v3i2.314
Vol 3 Issue 2 (2023)

Role of AI in cyber security through Anomaly detection and Predictive analysis

1 Deepshikha Aggarwal, 2 Deepti Sharma, 3 Archana B. Saxena
1 Jagan Institute of Management Studies, Rohini, Delhi, India
2 Jagan Institute of Management Studies, Rohini, Delhi, India
3 Jagan Institute of Management Studies, Rohini, Delhi, India

ABSTRACT

AI plays an essential role in improving cybersecurity by providing advanced tools and techniques to detect, prevent, and respond to cyber threats. It enables the development of algorithms that can recognize patterns of potential security breaches. Furthermore, AI can automate mundane tasks, and help identify and remediate vulnerabilities. Additionally, it can provide real-time threat intelligence and automated incident handling to facilitate faster detection and containment of threats. In this way, AI strengthens cybersecurity defences and prevents potential breaches. AI helps in enhancing cybersecurity by offering advanced tools and techniques for detecting, preventing, and responding to cyber threats. By developing algorithms, AI can identify patterns of possible security breaches. Moreover, it automates repetitive tasks and assists in identifying and resolving vulnerabilities. Additionally, AI enables real-time threat intelligence and automated incident handling, which helps in promptly detecting and containing threats. Through these capabilities, AI reinforces cybersecurity defences, minimizing the risk of potential breaches.AI plays an essential role in improving cybersecurity by providing advanced tools and techniques to detect, prevent, and respond to cyber threats. It enables the development of algorithms that can recognize patterns of potential security breaches. Furthermore, AI can automate mundane tasks, and help identify and remediate vulnerabilities. Additionally, it can provide real-time threat intelligence and automated incident handling to facilitate faster detection and containment of threats. In this way, AI strengthens cybersecurity defences and prevents potential breaches. AI helps in enhancing cybersecurity by offering advanced tools and techniques for detecting, preventing, and responding to cyber threats. By developing algorithms, AI can identify patterns of possible security breaches. Moreover, it automates repetitive tasks and assists in identifying and resolving vulnerabilities.

KEYWORDS:- Artificial intelligence, cyber security, anomaly detection, predictive analysis

INTRODUCTION

AI (Artificial Intelligence) plays a crucial role in enhancing cybersecurity by providing advanced tools and techniques to detect, prevent, and respond to cyber threats. Here are several ways in which AI can help in cybersecurity:

- Threat Detection and Analysis: AI algorithms can analyse network traffic, system logs, and user behaviour to identify unusual or suspicious patterns that may indicate a cyberattack. AI can be used to develop and update signature databases for known malware and vulnerabilities, aiding in the identification of threats.
- Predictive Analytics: AI can use historical data to predict potential security threats or vulnerabilities, allowing organizations to take proactive measures to mitigate risks.
- Real-time Monitoring: AI-powered security systems can continuously monitor networks and systems in real-time, swiftly identifying and responding to potential threats.
- User and Entity Behaviour Analytics (UEBA): AI can analyse user and entity behaviour to detect unusual or risky actions, helping organizations prevent insider threats and unauthorized access.
- Natural Language Processing (NLP): NLP can be used to scan and analyse text-based data sources like emails and chat logs to identify phishing attempts and other social engineering attacks.
- Malware Detection: Machine learning models can detect new and evolving malware strains by analysing code or behaviour, even without prior knowledge of the specific malware.
- Vulnerability Assessment: AI can assist in identifying and prioritizing system vulnerabilities by scanning code and configurations for potential weaknesses.
- Security Automation: AI can automate routine security tasks, such as patch management and log analysis, reducing the workload on security teams.
- Response and Recovery: AI can assist in incident response by providing recommendations for mitigating and recovering from security incidents.
- Security Awareness and Training: AI-powered simulations and training modules can help employees recognize and respond to security threats effectively.

Journal of Informatics Education and Research
ISSN: 1526-4726
https://doi.org/10.52783/jier.v3i2.314
Vol 3 Issue 2 (2023)

- Phishing Detection: AI can analyse email content and sender behaviour to identify phishing emails and provide alerts or block malicious content.
- Access Control and Identity Management: AI can enhance access control by continuously assessing user access and adjusting permissions based on user behaviour and risk.
- Network Security: AI can monitor network traffic for anomalies, helping to identify intrusion attempts and unauthorized access.
- IoT Security: AI can protect IoT devices by monitoring their behaviour and detecting abnormal activity, preventing potential attacks originating from these devices.
- Zero-day Threat Detection: AI can identify previously unknown vulnerabilities and threats by detecting unusual patterns or behaviours in applications or systems.
- Cloud Security: AI can enhance cloud security by continuously monitoring cloud environments for security issues and automating responses to threats.

While AI has numerous benefits in cybersecurity, it's essential to note that it is not a silver bullet and should be used in conjunction with other security measures and human expertise. Additionally, adversaries may also employ AI to enhance their attack methods, making the ongoing development of AI-driven cybersecurity solutions crucial in the ever-evolving landscape of cyber threats.

ROLE OF AI IN ANOMALY DETECTION

AI plays a critical role in anomaly detection for cyber-attacks by leveraging machine learning and data analysis techniques to identify deviations from normal patterns in network traffic, system behaviour, or user activity. AI systems collect and analyse vast amounts of data from various sources, including network logs, system logs, user behaviour, and application activity. Initially, AI models create a baseline of what is considered normal behaviour. This is done by analysing historical data to understand regular patterns and activities within the network or system. The AI system identifies relevant features or attributes from the data, such as the frequency of certain events, network traffic volume, user login patterns, and application behaviour. AI uses machine learning algorithms, such as clustering, decision trees, or neural networks, to model and learn the normal behaviour of the system. These models are trained on historical data and adapt over time. Once the AI system has learned what is normal, it continuously monitors incoming data and looks for deviations from the established baseline. When it detects patterns that significantly differ from the norm, it flags them as anomalies.

AI can handle vast amounts of data and is capable of scaling to monitor large and complex environments, which would be challenging for manual analysis. AI can help reduce false positive alerts by understanding context and patterns, minimizing unnecessary alerts that can overwhelm security teams. AI goes beyond simple rule-based systems by analysing behaviour. It can identify not only known attack patterns but also unknown and zero-day threats based on anomalous behaviour. AI systems can provide real-time or near-real-time detection of anomalies, which is critical for responding to emerging threats promptly. AI models can adapt and retrain themselves as new data becomes available. This means they can learn from recent anomalies and continuously update the baseline of what is considered normal. AI can be used to track and analyse the behaviour of users and entities within a network, identifying unusual or high-risk actions that may indicate a cyberattack.

AI-based anomaly detection can be integrated with SIEM systems, enhancing the overall security infrastructure. AI-powered anomaly detection significantly enhances an organization's ability to identify and respond to cyber threats promptly. However, it's important to regularly evaluate and update AI models, as adversaries also evolve their tactics to avoid detection. Additionally, anomaly detection should be part of a comprehensive cybersecurity strategy that includes other security layers and human expertise.

AI-BASED PREDICTIVE ANALYSIS FOR CYBERSECURITY

AI-based predictive analysis for cybersecurity refers to the use of artificial intelligence and machine learning techniques to forecast and anticipate potential cyber threats, vulnerabilities, or security incidents. The goal of predictive analysis in cybersecurity is to proactively identify and mitigate risks before they manifest as actual security breaches. Predictive analysis relies on the collection of vast amounts of historical and real-time data, which can include network traffic, system logs, user behaviour, threat intelligence feeds, and more. Relevant features or attributes are extracted from the data to build a dataset for analysis. These features could include the frequency of specific events, patterns in network traffic, and user access behaviour. AI and machine learning models, such as regression, decision trees, support vector machines, or

neural networks, are used to analyse the data and generate predictive models. These models are trained on historical data to identify patterns and trends.

Once trained, the AI models can predict and forecast potential cyber threats or vulnerabilities. This includes predicting future attack vectors, identifying weak points in the security infrastructure, or forecasting trends in attack techniques. Predictive analysis often involves assigning risk scores to various aspects of the organization's security landscape, allowing security teams to prioritize their efforts in addressing the most critical areas. Predictive analysis can incorporate external threat intelligence data to enhance its predictions. By analysing threat feeds and trends, the AI system can better understand the current threat landscape. AI-based predictive analysis may incorporate user and entity behaviour analytics (UEBA) to identify unusual or risky behaviour that may indicate insider threats or unauthorized access. Predictive models can adapt and evolve as new data becomes available. This enables them to improve their accuracy over time and adapt to changing threats.

In some cases, predictive analysis can trigger automated responses or alerts when high-risk predictions are made. This can include actions like quarantining a suspicious device or alerting security personnel. AI-based predictive analysis can scale to monitor large and complex network environments, which would be challenging for manual analysis. In addition to predicting threats, AI can help in identifying the root causes of vulnerabilities or incidents, allowing organizations to address the underlying issues. AI-based predictive analysis is a proactive approach to cybersecurity, helping organizations stay ahead of evolving threats and vulnerabilities. It complements traditional cybersecurity practices such as signature-based detection and reactive incident response, enabling a more comprehensive and forward-looking security posture. However, it's important to remember that predictive analysis is not fool proof and should be used in conjunction with other cybersecurity strategies and human expertise.

CONCLUSION

AI (Artificial Intelligence) plays a crucial role in enhancing cybersecurity by providing advanced tools and techniques to detect, prevent, and respond to cyber threats.AI enables the development of sophisticated algorithms that can analyse vast amounts of data and identify patterns that indicate potential security breaches. These algorithms can quickly identify and categorize threats, allowing security teams to prioritize and respond effectively. By constantly learning and adapting to new threats, AI systems can stay one step ahead of cybercriminals. Furthermore, AI can also automate repetitive tasks such as patching vulnerabilities and configuring firewalls, freeing up human resources for more strategic activities. With AI, businesses can significantly strengthen their cybersecurity defences and mitigate the risks posed by evolving cyber threats.AI (Artificial Intelligence) plays a crucial role in enhancing cybersecurity by providing advanced tools and techniques to detect, prevent, and respond to cyber threats. AI enables the development of sophisticated algorithms that can analyse vast amounts of data and identify patterns that indicate potential security breaches. These algorithms can quickly identify and categorize threats, allowing security teams to prioritize and respond effectively. By constantly learning and adapting to new threats, AI systems can stay one step ahead of cybercriminals. Furthermore, AI can also automate repetitive tasks such as patching vulnerabilities and configuring firewalls, freeing up human resources for more strategic activities. With AI, businesses can significantly strengthen their cybersecurity defences and mitigate the risks posed by evolving cyber threats.

AI can also help in the identification and remediation of vulnerabilities. By analysing network traffic and system logs, AI can pinpoint potential weaknesses and recommend appropriate patches or updates. This proactive approach can prevent potential breaches before they occur. Additionally, AI can assist in incident response by providing real-time threat intelligence and automated incident handling. This allows for faster detection and containment of threats, minimizing the impact on the organization. Overall, AI's capabilities in cybersecurity are invaluable in the ever-evolving landscape of cyber threats. It empowers organizations to stay ahead of the curve and protect their sensitive data and systems.

REFERENCES

Aggarwal D. (2023), Green Education: A Sustainable Development Initiative with the Power of Artificial Intelligence (AI), Journal of Image Processing and Intelligent Remote Sensing, ISSN 2815-0953

Aggarwal D. (2018), Using the Technology Acceptance Model to Understand the Use of Bring Your Own Device (BYOD) to Classroom, Journal on Today’s Ideas - Tomorrow’s Technologies

Aggarwal D. ((2017), Supporting BYOD (Bring Your Own Device) in an Educational Campus through MANET, International Journal of Engineering and Management Research, Volume-7, Issue-4.

Aggarwal D. (2021). A Pragmatic Approach to the Usage of Digital Devices in Education in Developing Countries", in Turkish Journal of Computer and Mathematics Education (SCOPUS), Vol.12 No.13.

Aggarwal D. (2023). Integration of Innovative Technological Developments and AI with Education for an Adaptive Learning Pedagogy. China Petroleum Processing and Petrochemical Technology, Volume 23, Issue 2

Deepshikha Aggarwal. (2023). Green Education for a Sustainable Future. Journal of Environmental Impact and Management Policy (JEIMP) ISSN: 2799-113X, 3(04), 27–30. https://doi.org/10.55529/jeimp.34.27.30

Aggarwal, D., Sharma, D., & Saxena, A. B. (2023). Exploring the Role of Artificial Intelligence for Augmentation of Adaptable Sustainable Education. Asian Journal of Advanced Research and Reports, 17(11), 179–184. https://doi.org/10.9734/ajarr/2023/v17i11563

Aggarwal, D., Sharma, D., & Saxena, A. B. (2023). Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN).

Sheptunov, S.A.; Sukhanova, N.V. The Problems of Design and Application of Switching Neural Networks in Creation of Artificial Intelligence. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2020; pp. 428–431.2.

Kim, M.S. The Design of Industrial Security Tasks and Capabilities Required in Industrial Site. In Proceedings of the 202121st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter, Ho Chi Minh City, Vietnam, 28–30 January 2021; ACIS International: Mt.Pleasant, MI, USA, 2021; pp. 218–223

Hu, Z.; Chiong, R.; Pranata, I.; Bao, Y.; Lin, Y. Malicious web domain identification using online credibility and performance data by considering the class imbalance issue. Ind. Manag. Data Syst. 2019, 119, 676–696

Hong, T.; Hofmann, A. Data Integrity Attacks against Outage Management Systems. IEEE Trans. Eng. Manag. 2021