SHODH SAGAR ®
Journal of Artificial Intelligence and Machine Learning
Vol. 1 | Issue 2 | Apr - Jun 2024 | Peer Reviewed & Refereed

AI-Enhanced Cyber Threat Detection and Response Systems

Sumit KR Sharma*
Defence Institute of Advanced Technology (DRDO), Pune
Email - sk.brave.124@gmail.com
ORCID: https://orcid.org/0000-0001-6546-0348

Accepted: 10/05/2024 Published:30/06/2024 * Corresponding author

How to Cite this Article:
Sharma, S. K. (2024). AI-Enhanced Cyber Threat Detection and Response Systems. *Shodh Sagar Journal of Artificial Intelligence and Machine Learning*, 1(2), 43-48.
DOI: https://doi.org/10.36676/ssjaiml.v1.i2.14

Abstract: *In this era of ubiquitous and highly developed cyber dangers, cybersecurity has emerged as an essential issue for modern organisations. Interest in using AI to improve cyber threat detection and response skills is on the rise as conventional approaches fall behind the dynamic threat environment. Recent advancements, problems, and future prospects are highlighted in this review paper's thorough overview of cyber threat detection and response systems augmented with AI. At the outset, we cover the basics of artificial intelligence (AI) in cybersecurity and trace the development of systems to identify cyber threats. We continue by outlining the benefits and drawbacks of supervised, unsupervised, and reinforcement learning, three of the AI-driven threat detection methods now available. Here, we show how AI-powered systems may effectively mitigate cyber risks in many sectors using real-world applications and case studies. Data quality, adversarial assaults, and ethical issues are just a few of the constraints and problems that we highlight and provide solutions for. Lastly, we go into the latest developments and potential paths forward in AI-powered cybersecurity, highlighting the need of working together across disciplines and continuously doing research to keep up with ever-changing threats. Researchers, practitioners, and policymakers may use this paper as a guide to better understand AI in cybersecurity, where it is now, and how to make future breakthroughs.*

Keywords: Cybersecurity, Artificial Intelligence, Threat Detection, Response Systems, Machine Learning, Deep Learning, Supervised Learning, Unsupervised Learning, Reinforcement Learning

Introduction

The development of cyber attacks poses major dangers to data integrity, privacy, and operational continuity, making cybersecurity an essential issue for organisations globally in the digital age. Conventional cybersecurity procedures are finding it harder and harder to keep up with the ever-changing tactics and strategies used by attackers. As a result, there is a growing movement to strengthen cyber threat detection and response systems by using AI. We will delve

into the development, fundamental ideas, and practical applications of AI-enhanced cyber threat detection and response systems in this thorough investigation. We find the need of AI integration in current cybersecurity paradigms by following the evolution of cyber threat identification from signature-based methods to AI-driven solutions. The story takes place in the midst of rising cyber dangers, and AI is seen as a potential friend in the never-ending fight to protect digital assets and infrastructure. By analysing current trends, obstacles, and anticipated future developments, this paper seeks to shed light on the revolutionary power of AI in bolstering cyber defences and reducing the dynamic nature of cyber threats.

Review literature

(Thapa & Arjunan, 2018) studied "ai-driven threat detection and response: a paradigm shift in cybersecurity" and said that This study delves into the topic of artificial intelligence (AI) and its use in cybersecurity, discussing its relevance, difficulties, and potential future developments, with a focus on its critical function in detecting and responding to threats.

(Stroup et al., 2019) studied "Application of AI in the NAS – the Rationale for AI-Enhanced Airspace Management" and said that In order to handle operational issues including traffic flow management, UMATM integration, fair access, and information exchange networks, this article investigates the need of artificial intelligence (AI) in the National Airspace System.

(Yaseen, 2023) studied "ai-driven threat detection and response: a paradigm shift in cybersecurity" and said that This study delves into the topic of artificial intelligence (AI) and its use in cybersecurity, discussing its relevance, difficulties, and potential future developments, with a focus on its critical function in detecting and responding to threats.

(Chahal, 2023) studied "AI-Enhanced Cyber Incident Response and Recovery" and said that Integrating sophisticated technologies, addressing ethical challenges, and improving cybersecurity outcomes by boosting threat detection speed and minimising false positives are the goals of the AI-enhanced Cyber Incident Response and Recovery initiative.

(Kumar et al., 2023) studied "Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era" and said that Artificial intelligence's (AI) capacity to swiftly handle and analyse massive volumes of data is the focus of this study as it explores AI's revolutionary role in cyber security. It stresses the need of strong governance systems and human monitoring to guarantee ethical concerns and effective actions. Additional conversations on the function of AI in cyber defence are laid out in the article.

(Alevizos & Dekker, 2024) studied "Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline" and said that This article delves at the possibility of automated mitigation suggestions and real-time insights that might result from integrating AI with conventional cyber threat intelligence (CTI) methodologies. Nevertheless, concerns about prejudice, lack of transparency, and ethical quandaries persist.

(Arif et al., 2024) studied "Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research" and said that This article provides a comprehensive overview of cloud threat detection with an emphasis on how AI has developed and how it may revolutionise cyber security. Case studies, ethical issues, and the need of a team

effort to resolve privacy, prejudice, and responsibility are all covered. In its whole, the article argues for a method that integrates AI with human knowledge.

(Chukwu et al., 2024) studied "Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration" and said that The need for artificial intelligence and machine learning in supply chain management has been magnified because of the COVID-19 epidemic. Integrating AI, especially for cost optimisation and real-time monitoring, greatly improves security, according to a poll of 281 managers. But there are obstacles to broad adoption, such as high adoption prices and a lack of trained staff. Some suggestions include security systems that are both affordable and allow for real-time tracking.

(Kuttiyappan & V, 2024) studied "AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis" and said that Methods for detecting fraud using artificial intelligence are the subject of this study. Specifically, the authors examine Temporal Convolutional Networks, Generative Adversarial Networks, and Graph Neural Networks. Using benchmarks like as logistic regression, random forest models, and conventional rule-based systems, it assesses how well these newer techniques perform.

Evolution of Cyber Threat Detection Systems

Thanks in large part to developments in AI and ML, cyber threat detection systems have undergone a gradual transition away from conventional signature-based techniques and towards more dynamic and adaptable ones. At first, signature-based approaches were the mainstay of cyber threat identification. These methods included searching through system logs and network traffic for recognised patterns or signatures of harmful code or behaviours. The fast development of new and polymorphic malware types made it difficult for existing technologies to stay up, even while they worked well against recognised threats. As a result, tactics that are more proactive and dynamic and can identify risks that were previously undetected are necessary. Anomaly detection methods were born out of this need to find suspicious patterns of system behaviour that might indicate a security breach. On the other hand, early anomaly detection systems were not very scalable and often had significant false positive rates. A new age in cyber threat detection has begun with the development of AI and ML, which allow for the use of complex algorithms that can learn from massive amounts of data in order to identify trends and outliers. To properly categorise and identify known risks, models may be trained on labelled datasets using supervised learning methods, for example. Conversely, by recognising patterns of behaviour that differ from the usual, unsupervised learning approaches enable the discovery of new or unknown dangers. Furthermore, reinforcement learning has shown potential in facilitating autonomous and adaptive threat response systems. The importance of artificial intelligence and machine learning in bolstering defences against a wide variety of cyber attacks has been highlighted by the development of cyber threat detection systems.

Fundamentals of AI in Cybersecurity

A wide variety of approaches and procedures are at the heart of artificial intelligence (AI) in cybersecurity, with the overarching goal of improving cyber threat detection, prevention, and mitigation. Artificial intelligence (AI) is based on the idea that computers can learn and make decisions in a way that is similar to a human. Applying AI approaches to cybersecurity involves sifting through massive amounts of data in search of patterns and anomalies that might indicate hostile behaviour. Machine learning (ML) is an essential component of artificial intelligence (AI) for cybersecurity. It includes many algorithms and techniques that allow systems to better themselves over time by learning from data, all without human intervention or programming. In applications like malware detection and classification, when labelled datasets are available for training, supervised learning methods like decision trees and support vector machines (SVMs) are widely used. Clustering and anomaly detection are two examples of unsupervised learning approaches that may be used to find risks and unusual behaviour in system logs or network traffic that were not there before. A branch of machine learning, deep learning has recently become an effective tool in cybersecurity. By using neural networks, it can automatically derive hierarchical features from unstructured data and accomplish top-notch results in areas such as image recognition and NLP. Security alerts and threat intelligence reports are examples of textual data that may be analysed using natural language processing (NLP) methods. This allows for the extraction of actionable insights and the automation of decision-making processes. While reinforcement learning isn't often used in cybersecurity, it might be a game-changer for creating threat response systems that can learn and adapt in response to environmental input. In general, artificial intelligence (AI) as it pertains to cybersecurity is all about bringing together state-of-the-art tools and techniques to make cyber defence systems more effective and resilient against new and different types of attacks.

AI-Enhanced Threat Detection Approaches

The goal of various AI-enhanced threat detection technologies is to make cyber defence systems more effective and faster in detecting and preventing harmful activity. These methods make use of AI and ML to sift through mountains of data, look for trends, and spot outliers that might be signs of security breaches. The supervised learning method is well-known for its ability to accurately identify and categorise known dangers via the use of machine learning models trained on labelled datasets. Common supervised learning techniques used for applications like as malware detection and intrusion detection include support vector machines (SVMs), decision trees, and random forests. However, by recognising patterns of behaviour that differ from typical system activity, unsupervised learning approaches allow for the discovery of new or unknown dangers. When looking for unusual activity in system logs or network traffic, clustering methods like k-means and hierarchical clustering are often used. Another potent method for threat identification is deep learning, which uses neural networks to automatically derive hierarchical features from unstructured data and get top-tier results in areas like image recognition and NLP. Cybersecurity applications that rely on deep learning often use recurrent neural networks (RNNs) and convolutional neural networks (CNNs).

Furthermore, reinforcement learning shows potential for facilitating autonomous and adaptive threat response systems that grow and learn from environmental input. Organisations may build proactive cyber defence systems that can identify and react to a broad variety of cyber attacks in real-time by integrating these AI-enhanced threat detection technologies.

Real-World Applications and Case Studies

Case studies and real-world applications show how cyber threat detection and response systems augmented with AI may make a difference in many businesses and disciplines. One example is the use of artificial intelligence (AI) by banks and other financial organisations to safeguard client accounts against theft and identify fraudulent activities. Analysing transactional data in real-time, machine learning algorithms detect suspicious trends and indicate potentially fraudulent activity. This allows for quick intervention and mitigation, as shown in case studies. Cybersecurity solutions powered by artificial intelligence also protect medical equipment and personal patient information in the healthcare sector. To ensure the confidentiality and integrity of diagnostic information, case studies demonstrate how deep learning algorithms are used to identify abnormalities in medical imaging data. In addition, threat detection systems driven by AI are crucial in the defence and government sectors for protecting key infrastructure and national security from cyber assaults. Using sophisticated machine learning techniques, case studies show how to examine network data and spot possible dangers from cybercriminal syndicates or state-sponsored actors. Cybersecurity solutions that use AI also shield online retailers and e-commerce platforms against phishing and other cyberattacks that compromise sensitive consumer data and transaction records. In order to identify and prevent fraudulent or harmful connections or actions, case studies show how algorithms based on natural language processing (NLP) examine website content and email conversations. In sum, case studies and real-world applications show that cyber threat detection and response systems improved with AI are effective in protecting persons and organisations from a variety of cyber risks in today's interconnected digital environment.

Conclusion

AI integration in cybersecurity is a significant advancement, enabling accurate and speedy threat detection and response. However, challenges like data privacy, adversarial attacks, and ethical implications persist. Future research should focus on enhancing collaboration, exploring advanced models, and improving interpretability.

Reference

Alevizos, L., & Dekker, M. (2024). Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. Electronics, 13(11), 2021. https://doi.org/10.3390/electronics13112021

Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International

Journal of Multidisciplinary Sciences and Arts, 2(2), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452

Chahal, S. (2023). AI-Enhanced Cyber Incident Response and Recovery. International Journal of Science and Research (IJSR), 12(3), 1795–1801. https://doi.org/10.21275/SR231003163025

Chukwu, N., Yufenyuy, S., Ejiofor, E., Ekweli, D., Ogunleye, O., Clement, T., Obunadike, C., Adeniji, S., Elom, E., & Obunadike, C. (2024). Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration. International Journal of Scientific and Management Research, 07(03), 46–65. https://doi.org/10.37502/IJSMR.2024.7306

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. Journal of Computers, Mechanical and Management, 2(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

Kuttiyappan, D., & V, R. (2024). AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis. Proceedings of the 1st International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security, IACIDS 2023, 23-25 November 2023, Lavasa, Pune, India. Proceedings of the 1st International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security, IACIDS 2023, 23-25 November 2023, Lavasa, Pune, India, Lavasa, India. https://doi.org/10.4108/eai.23-11-2023.2343170

Pooja, & Shilpa. (2017). IMPLEMENTATION ON INTRUSION DETECTION SYSTEM IN MOBILE COMPUTING. International Journal for Research Publication and Seminar, 8(5), 9–13. Retrieved from https://jrps.shodhsagar.com/index.php/j/article/view/1048

Singh, S. (2017). Study of Security in Cloud computing. Universal Research Reports, 4(1), 22–30. Retrieved from https://urr.shodhsagar.com/index.php/j/article/view/25

Stroup, R. L., Niewoehner, K. R., Apaza, R. D., Mielke, D., & Maurer, N. (2019). Application of AI in the NAS – the Rationale for AI-Enhanced Airspace Management. 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), 1–10. https://doi.org/10.1109/DASC43569.2019.9081768

Thapa, P., & Arjunan, T. (n.d.). AI-Enhanced Cybersecurity: Machine Learning for Anomaly Detection in Cloud Computing.

Thapliyal, V., & Thapliyal, P. (2024). Machine Learning for Cybersecurity: Threat Detection, Prevention, and Response. Darpan International Research Analysis, 12(1), 1–7. https://doi.org/10.36676/dira.v12.i1.01

Yaseen, A. (n.d.). AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY.