Enhancing Cybersecurity with AI-Driven Anomaly Detection and Threat Analytics

Megha Jayamohan[1], Pooja Krishnan [2]

24su25443@mec.edu.om[1], pooja@mec.edu.om[2]

Department of Computing and Electronics, Middle East College, Muscat, Oman [1,2]

Abstract. This research explores how AI-driven anomaly detection enhances cybersecurity by identifying irregularities in user activity, network traffic, and system logs. Unlike traditional signature-based systems, AI models—particularly unsupervised and semi-supervised approaches—offer greater adaptability and precision in detecting emerging threats. The study evaluates these models' performance in recognizing behavioral deviations while addressing challenges such as high false positives and inconsistent data quality. Findings show that AI-based analytics significantly improve threat detection accuracy and operational efficiency. However, the opaque nature of deep learning models limits interpretability, prompting the need for explainable AI (XAI) to support analysts' understanding. The study concludes that AI-powered security analytics are essential for proactive threat management, with future work focusing on scalability, reducing false alerts, and enhancing visualization for effective human–AI collaboration.

Keywords: Anomaly Detection, Threat Detection, AI, Cybersecurity.

1 Introduction

Cybersecurity has emerged as a major concern with increasing number of people, businesses and governments using digital platforms for communication and storing data. This reliance exposes us to complex cyber threats. In such a scenario, traditional rule-based security systems are bound to fail. Artificial intelligence (AI) is a game changing technology that offers smart and dynamic solutions to strengthen digital defences. AI can be employed to take cybersecurity systems beyond reactive models to proactive and dynamic in real-time threat detection and removal [1].

To improve threat identification and automate response systems, AI leverages technologies such as Machine Learning, Deep learning, and Natural Language Processing. AI provides better speed and accuracy of detecting complex cyberattacks compared to traditional methods [1].

MECSRC 2025, May 01, Muscat, Oman

DOI 10.4108/eai.1-5-2025.2361306

AI powered Anomaly Detection

One of the most important applications of AI in security is anomaly detection. This involves the detection of behaviour, network activity, or system usage that falls outside an expected norm, potentially indicating a security compromise. Traditional systems rely almost exclusively on predefined rules, which means that their ability to detect new attacks is restricted by how well these can be predicted ahead of time. By comparison, AI-driven systems apply statistical and probabilistic methods to continually learn what "normal" looks like and spot tiny variations that may indicate harmful behaviour [2] [3].

For instance, supervised learning algorithms such as Support Vector Machines (SVMs) or Decision Trees may be trained on labelled data to distinguish between legitimate and malicious activity. Unsupervised models such as k-means clustering or autoencoders are especially useful when dealing with never-before-seen attack vectors. Architecture of deep learning like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can process huge volumes of data, recognize temporal patterns, and recognize abnormal patterns in event sequences [3], [4].

Hybrid methods that integrate two or more learning methods are highly efficient in removing false positives. Anomaly-based intrusion detection systems (IDS) based on AI, as presented by Shafi and Mirjat, are not only quicker but also flexible and more precise, and thus highly efficient in situations where network traffic patterns are constantly evolving [3].

Threat Analytics and Predictive Modelling

Threat analytics is the process of gathering, analyzing, and interpreting security information to define possible threats. AI revolutionizes threat analytics by making it possible for systems to identify threats in real-time, connect events from varied sources, and forecast attacks. Predictive modelling is very powerful as it revolutionizes cybersecurity from a reactive to a proactive practice.

By integrating historical data and real-time monitoring, predictive models driven by AI can anticipate attacks and send early alerts. A sample model, for instance, could identify a user reading files in a non-normal order or from an unexpected location and raise an alarm. Behavioural analytics can be leveraged to build rich user profiles and indicate off-pattern behaviour, assisting in detecting insider threats arguably the most challenging threat to spot.

Natural Language Processing (NLP) is also utilized to block malicious messages and detect phishing in messages and emails. According to Jada and Mayayise, AI systems with NLP functionalities can analyze email metadata, sentence structure, and even psychological indicators to identify phishing at high accuracy [5]. Foreseeing AI models are also of utmost significance in vulnerability management and threat hunting, allowing analysts to prioritize high-risk regions prior to vulnerability exploitation [6].

2 Literature Review

2.1 Case Studies

A few real-life applications show the strength of AI in cyber-security:

Financial Sector: Banks and other financial institutions make use of AI to identify and prevent frauds. In assessing patterns within transactional data, AI programs can identify deviations that suggest fraud. Dash et al. discovered that the systems minimized financial loss and maximized customer confidence [1]. Jada and Mayayise also illustrated how behavioural analysis maximizes fraud detection rates through learning characteristic spending behaviours [5]. Healthcare Sector: Hospitals and clinics use AI to protect confidential patient information. AI applications watch for user behaviours and flag unfamiliar ones, which help enforce health data protections such as HIPAA. Madupati said AI applications not only protect electronic health records but also have predictive notice of likely breaches based on the method users enter it [2]. Government Agencies: The government national security agencies use AI to carry out cyber intelligence and threat hunting. AI is employed to filter through big datasets to detect potential threats against public infrastructure. Shafi and Mirjat explained how national cyber defence agencies employ AI models to monitor cyber espionage and DDoS attack trends more effectively [3].

Enterprise Environments: Businesses employ AI-powered hybrid IDS products that integrate anomaly-based and signature-based detection to monitor network traffic and react in real-time to any malicious activity [3]. Hybrid solutions are well-suited to dynamic IT infrastructure environments where rule-based solutions would not be able to respond in a timely manner. An article in [2] explained how a small firm deployed a light-weighted AI solution to track endpoint activity and observed a 65% drop in malware infection in a span of six months—testifying to the cost savings and scalability of AI when well adjusted.

2.2 Challenges

Although AI improves cybersecurity strength, it also comes with its own challenges. One of the main challenges is the vulnerability of AI models to adversarial attacks. During adversarial attacks, the malicious attackers tamper with the input data in a way that the AI model makes incorrect choices without being suspicious. The tampering is subtle but powerful, and therefore the models become vulnerable [3], [7].

Another challenge is the problem of false positives and false negatives. While AI systems are more precise than their human counterparts, they are not perfect. False positives can flood security analysts with meaningless alerts, and false negatives can allow real threats to pass undetected.

AI systems need access to huge amounts of data to operate effectively. If not controlled, such data can be used in an unwanted manner or made open to attacks and therefore present additional threats to data privacy [8]. Algorithmic bias is also a risk where if biased data is utilized to train an AI system, the choices that it makes will reflect the bias.

Most AI models are black boxes, giving little insight into why they make a specific decision. The absence of transparency complicates trust and accountability. Explainable AI (XAI) is a

new discipline that tries to address this challenge. Malik believes that XAI gives complete reasons for every decision an AI system takes, boosting transparency and gaining the trust of cybersecurity experts [6].

2.3 Future directions and Recommendations

To realize the ultimate potential of Artificial Intelligence in security, upcoming studies and development must concentrate on a series of strategic, technological, and moral enhancements:

Deployment of Explainable AI (XAI): The biggest need is to improve the transparency of AI systems. Explainable AI can bring forth a visible image of the decisions made by models in an understandable format to cybersecurity professionals, particularly in environments of high threat. Malik highlights that XAI enhances trust, supports auditing, and boosts accountability in automated systems for threat detection [6].

Fostering Proactive Defence through Predictive Analytics: Besides identifying threats, AI must also block them. Next-generation systems will use time-series analysis, context-aware threat intelligence, and past attack patterns to predict vulnerabilities. Predictive AI models can be trained to make decisions on vulnerable points in a system before they are exploited for teams to react before breaches are made [1].

Tailor-Made AI Solutions for SMEs: While larger corporations may have the means to maintain sophisticated AI infrastructure, smaller and medium businesses (SMEs) are weighed down by expense and expertise. Joshua and Mylavarapu propose that scalable, lightweight security frameworks should be designed to accommodate organizations with limited computational resources [7].

Human-AI Collaboration and Training: AI ought to support and augment human decision-making. The future work will need to prioritize the development of interfaces that simplify cybersecurity analysts' interpretation of AI output. Jada and Mayayise recommend frequent training schemes that prepare security teams to interpret and work alongside AI systems in a better way [5].

Continued Study on AI Defence against Adversaries: AI evolves, and so does the modus operandi of the culprits. Adversarial AI is a developing menace where the culprits tamper with data to mislead AI models. Shafi and Mirjat recommend studies in resilient models that can identify and counter adversarial inputs to maintain integrity and precision [3].

By investing in these areas, the cyber security community can make AI-driven systems more secure, scalable, and useful thus ensuring a safer digital future.

3 Conclusion

Artificial Intelligence is not just a technical innovation in cybersecurity; it is an evolution. As cyber threats grow more sophisticated and frequent, the demand for AI grows more imperative to maintain the digital world secure and resilient. AI allows systems to move beyond passive defence into active measures with real-time threat detection, predictive analysis, and automated incident response. It works particularly well for identifying patterns humans might miss and responding to dangers that happen faster than human capability.

But integrating AI into cybersecurity has its problems. Data privacy, explainability, resource requirements, and adversarial attacks are among the challenges which still plague the integration. All these challenges reinforce the need for explainable AI, human-AI collaboration, and ethical design. For AI to become an integral friend of cybersecurity, it must be transparent, equitable, and inclusive—qualities attainable only by sustained research and development.

In the future, collaboration between governments, academicians, and industry stakeholders will be needed to establish standards, improve the accessibility of AI, and establish safe practices. With human judgment overlaid onto it and imbued with sound ethics, AI not only can detect and prevent threats but create a better, safer cyber space for everyone. The cybersecurity future isn't just AI-enabled—it is AI-facilitated.

References

[1] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications, 13(5), 13–21. https://doi.org/10.5121/ijsea.2022.13502

[2] B. Madupati, "AI-Driven Threat Detection in Cybersecurity," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 2, no. 2, pp. 1163-1167, 2024. https://doi.org/10.2139/ssrn.5076610

[3] Shafi, M., & Mirjat, N. A. (2024) "Enhancing Cybersecurity with AI: From Anomaly Detection to Threat Mitigation." Journal for Multidisciplinary Research, vol. 1, no. 03, 2024, pp. 20-39. https://www.neliti.com/publications/590964/enhancing-cybersecurity-with-ai-from-anomaly-detection-to-threat-mitigation#cite

[4] Leong, W.Y., Leong, Y.Z., Leong, W.S. (2026). Artificial Intelligence-Driven Fraud Detection: Enhancing Security in Digital Age. In: Meen, TH., Yang, CF., Chang, CY. (eds) Proceedings of the 7th International Conference on Knowledge Innovation and Invention, Volume 1. ICKII 2024. Lecture Notes in Electrical Engineering, vol 1481. Springer, Singapore. https://doi.org/10.1007/978-981-95-2113-5_7

[5] Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

[6] S. Malik, "Explainable AI for Cybersecurity: Improving Transparency in Automated Threat Detection Systems," December 2024. [Online]. https://doi.org/10.13140/rg.2.2.14173.93927

[7] Joshua, N. E., & Mylavarapu, N. P. (2025). AI-driven threat detection: Enhancing cybersecurity automation for scalable security operations. International Journal of Science and Research Archive, 14(3), 681–704. https://doi.org/10.30574/ijsra.2025.14.3.0615

[8] Tarafdar, R. (2025). AI-powered cybersecurity threat detection in cloubd environments. International Journal of Computer Engineering & Technology, 16(1), 3858–3869. https://doi.org/10.34218/ijcet_16_01_266