

Midocean University

College of Informatics

Department of Artificial Intelligence



A LITERATURE REVIEW REPORT ON CYBERSECURITY AND THREAT DETECTION

Prepared by:

Sultan Khalaf Alotaibi (222000226)

Supervised by:

Dr.Mohammed Anbar

First semester 2025

Contents

Abstract	2
Summary of Research Papers	2
Critical Analysis.....	5
Connections.....	6
Conflicts Between the Findings	7
Synthesis Matrix for Literature Review:.....	8
References.....	10

Abstract

The fast-paced evolution of cybersecurity threats demands sophisticated detection methods and mitigation strategies to protect essential systems. The research paper examines six current studies that investigate AI, deep learning, and machine learning methodologies for detecting and responding to threats. The research examines AI security frameworks alongside deep learning methods, mechanisms for detecting internal threats and applications of NLP within cybersecurity. Research findings demonstrate AI systems excel at anomaly detection while simultaneously reducing insider threats and streamlining automated responses. Despite advancements in AI and machine learning techniques for threat detection ongoing challenges include false positives together with ethical concerns and real-world validation needs.

Summary of Research Papers

Paper 1: AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY (Yaseen, 2023)

The research demonstrates how AI transforms cybersecurity through advanced prediction tools and swift threat response capabilities. The paper evaluates traditional cybersecurity methods alongside AI-based solutions that deploy machine learning algorithms for detecting and responding to threats in real time. The research identifies essential challenges which consist of ethical considerations along with biases in AI models and the potential for adversarial attacks. AI-driven cybersecurity systems promise major improvements in reducing false positives and automation while requiring human supervision to maintain dependable decision-making and address AI vulnerabilities.

**Paper 2: CYBER SECURITY THREATS DETECTION IN INTERNET OF THINGS
USING DEEP LEARNING APPROACH (Ullah et al., 2019)**

This research introduces a deep learning-based method for identifying cybersecurity threats in IoT systems. The research introduces a method which utilizes CNNs alongside TensorFlow deep neural networks to identify malware infections and unauthorized software changes within IoT systems. The paper evaluates the proposed model's effectiveness by testing it against datasets that include both malware samples and network traffic logs. Deep learning enhances threat detection accuracy in cybersecurity yet faces significant challenges regarding computational expenses and real-time operation within IoT systems with limited capabilities.

**Paper 3: DEEP LEARNING FOR UNSUPERVISED INSIDER THREAT DETECTION IN
STRUCTURED CYBERSECURITY DATA STREAMS (Tuor et al., 2017)**

The presented research paper details an unsupervised deep learning solution aimed at identifying insider threats in organizational network systems. The study utilizes system logs combined with anomaly detection methods to track user behavior and pinpoint actions that signify insider attacks. The research evaluates Deep Neural Networks (DNNs) against Recurrent Neural Networks (RNNs) and finds Recurrent Neural Networks (RNNs) outperform Deep Neural Networks (DNNs) in recognizing subtle anomalies. The model shows promise in identifying insider threats yet reveals the difficulty of achieving adversarial robustness while requiring implementation in real-world environments beyond synthetic data.

Paper 4: THREAT DETECTION AND RESPONSE USING AI AND NLP IN CYBERSECURITY(Ismail, 2024)

The study examines how Artificial Intelligence and Natural Language Processing techniques can enhance cybersecurity measures through phishing detection systems and automated threat responses. Researchers have demonstrated how AI-based systems process extensive datasets of text documents to discover malicious intentions in email exchanges and online chats. The paper demonstrates how Natural Language Processing methods perform effectively to remove spam and detect social engineering attacks while improving threat intelligence capabilities. According to the research findings AI explanation difficulties and dataset biases remain significant issues alongside the requirement for real-time adjustments to emerging cyber threats.

Paper 5: ENHANCING CYBERSECURITY: THE POWER OF ARTIFICIAL INTELLIGENCE IN THREAT DETECTION AND PREVENTION(Rizvi, 2023)

The analysis in this paper focuses on AI applications for cybersecurity enhancement through automated response operations and predictive analysis of threats. The research demonstrates how AI can analyze large volumes of data instantly to detect cyber threats in advance before they grow worse. AI excels in identifying zero-day vulnerabilities and adapting to advanced attacks through machine learning capabilities. The research identifies AI's cybersecurity limitations which involve transparency problems, ethical questions and necessary strong governance systems to avoid security flaws created by AI technology.

Paper 6: MACHINE LEARNING IN CYBERSECURITY: A REVIEW OF THREAT DETECTION AND DEFENSE MECHANISMS(Abrahams et al., 2024)

The research paper offers a thorough examination of machine learning methods for cybersecurity while organizing these approaches into supervised learning techniques, unsupervised learning methods, and reinforcement learning strategies. The study demonstrates how anomaly detection along with behavior analysis functions as critical methods for the prevention of cyber threats. The analysis shows machine learning models can detect malicious activities yet points out their weaknesses when attackers use adversarial techniques to alter data inputs and avoid discovery. The study recommends enhancements to machine learning methods through strengthening adversarial robustness capabilities while eliminating dataset biases and combining these methods with conventional cybersecurity defenses.

Critical Analysis

The assessed research introduces an all-encompassing method for detecting cybersecurity threats through AI algorithms and deep learning-based machine learning methodologies. These studies excel at detecting complex cyber threats accurately while they automate incident responses and adapt to new security risks in real-time. Cybersecurity frameworks benefit from improved phishing detection capabilities through the application of NLP techniques.

However, several limitations exist. The utilization of simulation-based testing limits applicability to the real world because real-world cybersecurity environments involve random variables and extremely sophisticated attackers. Further, ethical considerations of AI decision-making, bias in datasets, and susceptibility to adversarial manipulation demonstrate

the need for continual improvement of these methods. Most research focuses on specific threats like malware, phishing, or insider threats but does not consider a general cybersecurity approach with multiple attack surfaces simultaneously.

One of them is the computational overhead of deep learning models, which can prevent deployment in computation-limited setups like IoT networks. Future research should investigate compact models that provide a balance between computational efficiency and detection efficacy. In addition, the incorporation of AI with blockchain technology and human oversight mechanisms would increase trustworthiness and transparency of cybersecurity mechanisms.

Although these writings add significantly, their contrast with existing cybersecurity techniques must be more thorough to provide a better sense of the strengths and weaknesses of AI. Augmenting experimental verifications from simulations to actual-case investigations would also increase their real-world applicability.

Connections

1. **AI-Driven Cybersecurity:** All reviewed studies focus on leveraging AI and machine learning for cybersecurity threat detection and mitigation.
2. **Automated Threat Detection:** A common goal among the papers is the automation of cybersecurity defences to enhance real-time response mechanisms.
3. **Anomaly Detection and Behaviour Analysis:** Several papers emphasize the use of anomaly detection and behavioural analysis to identify threats, particularly insider threats and network intrusions.
4. **Real-Time Adaptation:** Most studies highlight the importance of cybersecurity systems that can adapt in real time to evolving cyber threats.

5. **Ethical and Computational Challenges:** Many studies acknowledge the challenges of AI biases, high computational costs, and adversarial threats.

Conflicts Between the Findings

1. **Supervised vs. Unsupervised Learning:** Some papers advocate for supervised learning techniques for threat detection, whereas others highlight the advantages of unsupervised learning for detecting novel threats.
2. **Traditional vs. AI-Powered Detection:** Some studies compare AI-based detection models with traditional cybersecurity techniques, showing varying degrees of improvement depending on the threat type.
3. **Network-Level vs. Device-Level Security:** While some papers focus on securing entire networks from cyber threats, others prioritize endpoint security to prevent malware and unauthorized access.
4. **Machine Learning vs. NLP-Based Security Models:** While some studies propose machine learning-based solutions, others emphasize the effectiveness of Natural Language Processing (NLP) in cybersecurity, particularly in phishing detection and text-based threat identification.
5. **Centralized vs. Decentralized Security Models:** Some research suggests centralized AI models for threat detection, while others advocate for decentralized, distributed approaches to reduce single points of failure and enhance system robustness.

Synthesis Matrix for Literature Review:

Study	Author s	Year	Research Design	Key Findings/Results	Methodology	Limitations
AI-driven threat detection and response: A paradigm shift in cybersecurity	Yaseen	2023	Theoretical Analysis and Case Study	AI-driven models enhance cybersecurity efficiency, reducing false positives and improving automation. However, ethical concerns and adversarial threats persist.	Comparative study of AI-based threat detection vs. traditional cybersecurity techniques	AI model bias, adversarial attacks, ethical concerns, and need for human oversight
Cybersecurity threats detection in internet of things using deep learning approach	Ullah et al.	2019	Experimental	Deep learning models, particularly CNNs, improve malware detection accuracy in IoT.	Implementation of deep learning models with real network traffic datasets	High computational cost, real-time constraints in IoT environments
Machine learning in cybersecurity : A review of threat detection and defence mechanisms	Okoli, et al.	2024	Literature Review & Experimental	Machine learning-based anomaly detection enhances cybersecurity but is susceptible to adversarial manipulation.	Categorization and performance assessment of ML threat detection techniques	Dataset biases, adversarial robustness, integration with traditional security frameworks
The power of artificial intelligence	Rizvi	2023	Review & Theoretical Analysis	AI enhances proactive threat detection,	Analysis of AI-driven security	AI transparency issues, ethical

in threat detection and prevention				improving predictive modeling and automated incident response.	models in cybersecurity frameworks	concerns, governance limitations
Threat Detection and Response Using AI and NLP in Cybersecurity	Ismail	2024	Experimental	NLP models improve phishing detection and enhance threat intelligence through text analysis.	Application of AI-driven NLP models on textual datasets (emails, chats)	AI explainability, dataset biases, need for real-time adaptability
Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams	Tuor et al.	2017	Experimental	RNN-based models outperform other deep learning approaches in detecting insider threats from system logs.	Anomaly detection and behaviour analysis using deep learning models	Limited real-world validation, adversarial robustness concerns

References

- Ismail, W. S. (2024). Threat Detection and Response Using AI and NLP in Cybersecurity. *J. Internet Serv. Inf. Secur.*, 14(1), 195-205. <https://jisis.org/wp-content/uploads/2024/03/2024.I1.013.pdf>
- Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 21(1), 2286-2295. <https://wjarr.co.in/wjarr-2024-0315>
- Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, 10(5), 055-060. https://www.academia.edu/download/102883869/IJAERS_08_may_2023.pdf
- Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017, February). Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams. In *AAAI Workshops* (pp. 224-231). <https://cdn.aaai.org/ocs/ws/ws0325/15126-68350-2-PB.pdf>
- Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cybersecurity threats detection in internet of things using deep learning approach. *IEEE access*, 7, 124379-124389. <https://ieeexplore.ieee.org/abstract/document/8812669/>

Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, 7(12), 25-43.

https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf