Enhancing Threat Detection with Artificial Intelligence and Machine Learning: A Comprehensive Analytical and Bibliometric Study

Students: Yasir Alalawi, Ajab Aldosari, Faisal Aldosari
Master of Artificial Intelligence,
Department of Computer Science,
prince sattam bin abdulaziz university

Abstract

The increasing sophistication of cyber threats has made artificial intelligence (AI) and machine learning (ML) critical for modern cybersecurity. This research integrates bibliometric and analytical perspectives to examine how AI and ML enhance threat detection, combining insights from five representative studies (2020–2025). Bibliometric analysis based on Web of Science data reveals dominant trends in deep learning, big data analytics, and explainable AI. Analytical comparison of algorithms across multiple datasets demonstrates the superiority of ensemble and deep learning models in identifying complex attacks. The findings indicate a strong research shift toward hybrid, interpretable, and data-driven security models. The paper concludes with recommendations for advancing scalable, explainable AI systems for proactive cybersecurity defense.

Keywords—Cybersecurity, Artificial Intelligence, Machine Learning, Threat Detection, Bibliometric Analysis, Deep Learning.

1. Introduction

Cybersecurity is evolving from static, rule-based systems to dynamic, AI-driven architectures capable of real-time adaptation and learning. As cyberattacks grow more complex, traditional intrusion detection systems (IDS) struggle to identify zero-day threats and advanced persistent attacks. Machine learning and deep learning methods enable the automatic extraction of patterns and anomalies from large-scale data, providing adaptive intelligence. This research aligns with the Advanced Concepts and Techniques of AI course, connecting theoretical AI foundations to practical cybersecurity applications. The objective is to explore the global research landscape, assess the performance of various AI/ML algorithms, and identify the leading directions in AI-powered threat detection.

2. Research Problem and Objectives

Despite the vast volume of data available for threat detection, most traditional systems are unable to handle the scale, complexity, and adaptability of evolving threats. AI and ML provide promising solutions, but challenges remain regarding model interpretability, computational efficiency, and resilience to adversarial attacks.

Objectives:
1. To analyze global research trends in AI and ML-based threat detection using bibliometric methods.

2. To compare the performance and methodologies of leading ML and DL algorithms across benchmark datasets.
3. To identify emerging themes such as explainable AI, federated learning, and hybrid models in cybersecurity.
4. To evaluate limitations, gaps, and future directions for AI-driven cybersecurity advancements.

3. Research Methodology

This study follows a hybrid research design combining bibliometric analysis with comparative algorithmic review. Bibliometric data were sourced conceptually from the Web of Science Core Collection to identify publication trends, keywords, and collaboration networks between 2020 and 2025. The proposed search query included ('artificial intelligence' OR 'machine learning') AND ('threat detection' OR 'cybersecurity'). Filtering criteria included English-language, peer-reviewed journal articles. Duplicate records would be removed, keywords normalized, and author data standardized. VOSviewer was designated for mapping co-authorship and keyword co-occurrence networks.

In parallel, five high-impact research papers were analyzed to represent empirical and conceptual perspectives. Three of these provided experimental data (Srinivasulu et al., Hemanth Kumar et al., Moustafa et al.), while two offered theoretical synthesis (Mohamed, Sharma et al.). This dual approach ensures both quantitative and qualitative evaluation of how AI and ML models enhance threat detection accuracy, scalability, and robustness.

4. Analysis Techniques

Performance indicators from the literature indicate deep learning and ensemble models outperform classical ML algorithms. Srinivasulu et al. (2025) demonstrated the effectiveness of CNNs for ransomware detection, while Hemanth Kumar et al. (2025) validated the superior accuracy of RNNs (96.8%) on big data cybersecurity datasets. Moustafa et al. (2025) extended this by benchmarking multiple ML algorithms (RF, SVM, Gradient Boosting, DNN) across fourteen datasets, where Random Forest achieved 98.2% accuracy with balanced trade-offs between precision and speed.

Sharma et al. (2025) emphasized inconsistencies in IDS evaluation standards, advocating for unified metrics (F1-score, ROC-AUC) and interpretability. Mohamed (2025) contributed to the conceptual understanding of emerging paradigms like Federated Learning, Explainable AI, and Quantum-AI convergence. These findings collectively demonstrate that hybrid models, which combine ensemble learning and deep neural networks, provide the most promising outcomes for modern cybersecurity frameworks.

5. Interpretation and Insights

Analysis of the five selected papers reveals consistent trends in the application of AI and ML for threat detection. Deep learning models such as CNNs and RNNs dominate due to their ability to learn temporal and spatial attack patterns, while ensemble models like Random Forest and Gradient Boosting offer interpretability and efficiency. Bibliometric evidence

supports a rapid increase in publications related to explainable and hybrid AI models between 2023 and 2025. This reflects a paradigm shift from purely accuracy-driven research to models prioritizing transparency, scalability, and adversarial resistance.

Paper	Focus	Key Insight	Limitation
Srinivasulu et al. (2025)	CNN-based threat detection	Deep learning models achieved >95% accuracy	Synthetic dataset
Mohamed (2025)	Review of AI paradigms	Introduced Explainable and Federated AI directions	Lacked quantitative validation
Hemanth Kumar et al. (2025)	Big Data + ML experiments	RNN achieved 96.8% accuracy; blockchain reduced false positives	High computational demand
Moustafa et al. (2025)	Comparative ML algorithms	RF and DNN performed best across 14 datasets	No real-time deployment tested
Sharma et al. (2025)	Survey of IDS algorithms	Hybrid CNN-LSTM reached up to 99% accuracy	Evaluation inconsistency across datasets

These studies collectively validate that AI and ML substantially enhance the precision, scalability, and adaptability of cybersecurity systems. The shift toward hybrid, explainable architectures marks a pivotal evolution in the field, indicating the maturity of AI-based defense systems.

6. Related Works

The selected literature provides comprehensive coverage of empirical, comparative, and conceptual research in AI-driven cybersecurity. The combination of deep learning, ensemble methods, and big data frameworks forms the foundation for the next generation of intelligent intrusion detection systems.

Author (Year)	Methodology	Findings	Limitations	Contribution
Srinivasulu et al. (2025)	Deep Learning CNN	High accuracy for ransomware detection	Synthetic dataset	Empirical demonstration of DL power

Mohamed (2025)	Systematic review	Explored Federated and Quantum AI	Lack of empirical data	Conceptual direction
Hemanth Kumar et al. (2025)	Big Data + ML	RNN achieved 96.8% accuracy	Computationally heavy	Applied perspective
Moustafa et al. (2025)	Comparative IDS benchmarking	RF achieved 98.2% accuracy; Gradient Boosting competitive	Imbalance sensitivity	Empirical cross-validation
Sharma et al. (2025)	Survey of ML/DL IDS algorithms	Hybrid CNN-LSTM models top performance	Evaluation inconsistency	Critical review of evaluation practices

7. Conclusion and Future Work

This comprehensive study confirms that Artificial Intelligence and Machine Learning play a transformative role in enhancing threat detection. Bibliometric trends reveal increasing collaboration and emphasis on Explainable and Federated AI between 2020 and 2025. Algorithmic analysis across five major studies highlights that deep and ensemble learning models outperform traditional methods in accuracy and adaptability.

Future research should focus on integrating explainability into high-performance models, addressing adversarial robustness, and reducing computational costs. Expanding analysis across Scopus and IEEE Xplore datasets would strengthen bibliometric precision and help identify emerging subfields like Reinforcement Learning-based cybersecurity.

References

[1] A. Srinivasulu et al., “Leveraging data analytics to revolutionize cybersecurity with machine learning and deep learning,” Scientific Reports, 2025.

[2] N. Mohamed, “Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms,” Knowledge and Information Systems, 2025.

[3] B. Hemanth Kumar et al., “Big Data in Cybersecurity: Enhancing Threat Detection with AI and ML,” Metallurgical and Materials Engineering, 2025.

[4] A. Moustafa et al., “Advanced IDS: A Comparative Study of Datasets and Machine Learning Algorithms for Network Intrusion Detection Based on Network Flows,” Applied Intelligence, 2025.

[5] P. Sharma et al., “Intrusion Detection in the Era of Machine Learning: A Critical Survey of Algorithms and Evaluation Practices,” International Journal of Computer Applications, 2025.