International Journal of Intelligent Computing and Security in Analytics and Applications (IJICAA)
Vol. 1, No. 1, May 2026 | e-ISSN: Applied For | Open Access

Intelligent Threat Detection Systems: A Survey of Machine Learning Approaches in Cybersecurity

Dhamodharan D
I M. Sc. Data Science
Department of computer Science and data science
Nehru Arts & Science College
Coimbatore, Tamil Nadu

Journal	IJICAA
Volume / Issue	Vol. 1, No. 1, May 2026
Pages	pp. 17–24
e-ISSN	Applied For
License	CC BY 4.0 Open Access

Abstract

The escalating sophistication of cyber threats has rendered traditional signature-based detection systems increasingly inadequate in protecting modern digital infrastructures. Machine learning (ML) and artificial intelligence (AI) have emerged as powerful enablers of intelligent threat detection, capable of identifying novel attack patterns through behavioral analysis and anomaly detection. This paper surveys ML-based approaches applied to cybersecurity threat detection, examining methodologies for intrusion detection, malware classification, phishing identification, and advanced persistent threat (APT) detection. We analyze the effectiveness of supervised classifiers, unsupervised anomaly detection algorithms, and deep learning models in processing network traffic, system logs, and endpoint telemetry data. The survey further addresses key challenges including adversarial machine learning, class imbalance, real-time processing requirements, and the interpretability of detection models in operational security contexts. Our findings indicate that ensemble methods and hybrid architectures combining signature-based and behavioral approaches yield superior detection performance compared to standalone models.

Keywords: *Cybersecurity, Threat Detection, Intrusion Detection Systems, Machine Learning, Anomaly Detection, Malware Classification*

1. Introduction

Cybersecurity threats have grown exponentially in both volume and sophistication, with adversaries employing advanced techniques including zero-day exploits, polymorphic malware, and coordinated multi-stage attacks. Traditional security mechanisms relying on static rule sets and known threat signatures fail to detect novel and evasive attack variants. The cybersecurity industry has consequently experienced increasing adoption of intelligent, data-driven detection methodologies capable of adapting to evolving threat landscapes.

Machine learning offers compelling capabilities for threat detection by learning statistical patterns associated with malicious activity from historical data. Unlike signature-based approaches, ML models can generalize learned patterns to previously unseen attack variants, enabling detection of zero-day threats. Furthermore, the ability to process high-velocity data streams from network sensors and endpoint agents enables real-time threat identification essential for minimizing breach impact.

This survey systematically examines ML methodologies applied to major cybersecurity threat detection domains, evaluating algorithm selection, feature engineering strategies, and performance metrics. The paper synthesizes findings from recent literature to provide a comprehensive reference for security researchers and practitioners.

2. Intrusion Detection Systems

Network intrusion detection systems (NIDS) monitor network traffic to identify malicious activities and policy violations. ML-based NIDS approaches analyze packet-level and flow-level features extracted from network captures to classify traffic as benign or malicious. Decision tree classifiers provide interpretable models suitable for operational deployment, while random forest ensembles demonstrate robust performance across diverse attack categories including port scanning, denial-of-service, and protocol exploitation.

Deep learning approaches, particularly autoencoders for unsupervised anomaly detection and recurrent neural networks for sequential traffic analysis, have demonstrated the ability to detect subtle behavioral anomalies indicative of advanced persistent threats. Graph-based neural network models that capture network topology and inter-host communication patterns represent an emerging research direction with promising detection capabilities.

3. Malware Detection and Classification

Malware detection represents one of the most extensively studied applications of ML in cybersecurity. Static analysis approaches extract features from binary files including byte n-grams, import tables, and control flow graphs, enabling classification without execution. Dynamic analysis methods analyze behavioral signatures captured during sandboxed execution, providing robustness against obfuscation techniques employed by sophisticated malware families.

Convolutional neural networks applied to malware binary visualizations have demonstrated state-of-the-art classification accuracy, leveraging spatial patterns in binary structure to distinguish malware families. Natural language processing techniques applied to disassembled code sequences enable semantic analysis of malware functionality beyond syntactic pattern matching.

4. Phishing and Social Engineering Detection

Phishing attacks targeting user credentials and financial information remain among the most prevalent cyber threats. ML-based phishing detection systems analyze URL characteristics, webpage content, visual similarity to legitimate sites, and email header metadata to identify fraudulent communications. Ensemble classifiers combining multiple feature modalities consistently outperform single-feature approaches.

Deep learning models trained on large-scale phishing datasets capture complex linguistic and visual patterns associated with deceptive content. Real-time URL analysis pipelines enable browser-integrated protection mechanisms that evaluate phishing probability before page loading.

5. Challenges in ML-Based Threat Detection

Several significant challenges constrain the effectiveness of ML-based security systems. Adversarial machine learning poses a fundamental threat, as sophisticated attackers can craft inputs designed to evade detection by exploiting model decision boundaries. Class imbalance in security datasets, where malicious samples constitute a small fraction of total observations, degrades classifier performance on minority threat classes. The requirement for real-time detection in high-throughput network environments constrains model complexity and inference latency. Model interpretability remains critical for security analysts who require explanations of detection decisions to support incident response.

6. Conclusion

ML-based threat detection represents a significant advancement over traditional signature-based approaches, offering adaptive capabilities essential for addressing evolving cyber threats. This survey has examined methodologies across intrusion detection, malware classification, and phishing detection, identifying ensemble and

hybrid approaches as consistently high-performing. Addressing adversarial robustness, interpretability, and operational efficiency represents the critical research agenda for advancing intelligent cybersecurity systems.

References

[1] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[2] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.

[3] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305-316.

[4] Vinayakumar, R., et al. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550.

[5] Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. ACM Computing Surveys, 50(3), 1-40.