MANTECH Publications

Journal of Computer, Internet and Network Security
Volume 10, Issue 3, September- December, 2025
ISSN: 2457-0176 (Online)

AI/ML-Driven Intrusion Detection and Threat Prediction for Intelligent Cybersecurity Management in Next-Generation Networks

Dr. Rajesh Rawat[1], Sheetal Rastogi[2], Kusum Pathak[3]

Associate Professor[1], Students[2, 3]

Department of Computer Science and Engineering

Indian Institute of Technology, Delhi

Email ID: *sheetal.rastogi404@gmail.com[2]*

ABSTRACT

The rapid evolution of digital infrastructures and the exponential growth of connected devices have dramatically increased the surface area for cyber threats. Traditional security systems, largely rule-based and reactive, are struggling to combat increasingly sophisticated cyberattacks. Artificial Intelligence (AI) and Machine Learning (ML) are transforming the field of cybersecurity by enabling proactive, adaptive, and intelligent threat detection mechanisms. This paper presents an in-depth exploration of AI/ML-driven intrusion detection and threat prediction systems, highlighting their methodologies, models, challenges, and future prospects. The study emphasizes how AI-based systems enhance network resilience through real-time anomaly detection, pattern recognition, and predictive analytics. Additionally, this paper discusses various challenges such as data imbalance, adversarial attacks, explainability, and computational overhead while outlining future research directions to advance intelligent cybersecurity defense mechanisms.

KEYWORDS: *Artificial Intelligence, Machine Learning, Intrusion Detection System, Threat Prediction, Cybersecurity, Anomaly Detection, Deep Learning, Network Security*

INTRODUCTION

In the digital era, the increasing dependency on interconnected systems, cloud infrastructures, and IoT networks has introduced unprecedented levels of cyber vulnerability. Traditional intrusion detection systems (IDS) rely heavily on signature-based approaches, which are efficient for known threats but fail against new and evolving attacks. Modern adversaries employ polymorphic and adaptive techniques that bypass static defense mechanisms.

AI and ML technologies are revolutionizing cybersecurity by offering systems that can learn from data, detect anomalies, and predict potential intrusions before they occur. These intelligent systems adapt to changing network behaviors, making them more suitable for dynamic environments. AI/ML-driven IDS not only detect threats but also predict attack vectors and adapt defense strategies autonomously.

This paper examines how AI and ML methods contribute to the development of smart, predictive, and self-learning intrusion detection systems capable of addressing contemporary cybersecurity challenges.

LITERATURE REVIEW

Traditional Intrusion Detection Systems (IDS)

Conventional IDS are primarily categorized into signature-based and anomaly-based systems. Signature-based IDS match traffic patterns against known attack signatures but fail to detect zero-day exploits. Anomaly-based IDS identify deviations from normal behavior but often suffer from high false-positive rates. These limitations prompted researchers to explore AI and ML approaches for more adaptive threat detection.

Evolution Towards AI and ML-Based Security Systems

Recent literature demonstrates a paradigm shift toward intelligent systems that leverage AI techniques. Machine learning algorithms such as Decision Trees, Random Forests, Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) have been applied for intrusion detection due to their pattern recognition capabilities. Deep learning models such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have shown superior performance in identifying complex attack patterns within massive datasets.

Hybrid and Ensemble Models

Researchers have also explored hybrid approaches that combine signature-based detection with anomaly detection powered by ML. Ensemble models integrate multiple classifiers to enhance detection accuracy. These systems benefit from both speed and adaptability, offering robust protection against both known and emerging threats.

Recent Developments in Threat Prediction

AI models are now being used for predictive threat intelligence. By analyzing historical data and attack trends, predictive systems can forecast potential security incidents. Reinforcement learning and generative models such as GANs (Generative Adversarial Networks) are increasingly used to simulate attacks and strengthen defensive models through adversarial training.

Table 1: Comparison Between Traditional and AI/ML-Based Intrusion Detection Systems

Feature	Traditional IDS	AI/ML-Based IDS
Detection Approach	Signature-based and rule-based	Data-driven and adaptive
Capability Against Zero-Day Attacks	Limited	High (predictive capability)
Learning Ability	Static	Continuous learning
False Positive Rate	High	Moderate to Low (after model training)
Response Time	Reactive	Proactive and automated
Maintenance	Manual updates required	Self-updating through retraining

AI/ML TECHNIQUES IN INTRUSION DETECTION

Supervised Learning Models

Supervised algorithms require labeled datasets to train detection models. Algorithms like SVM, Random Forest, and Gradient Boosting are widely used to classify network traffic into benign or malicious categories. While effective, they rely heavily on high-quality, labeled datasets, which can be difficult to obtain.

Table 2: Machine Learning Algorithms Used in Intrusion Detection Systems

Algorithm Type	Example Algorithms	Advantages	Limitations
Supervised Learning	Random Forest, SVM, Decision Tree	High accuracy on labeled data	Requires large labeled datasets
Unsupervised Learning	K-Means, DBSCAN, Autoencoder	Useful for unknown attacks	May have high false alarms
Deep Learning	CNN, LSTM, Autoencoders	Automatic feature extraction, scalable	High computational cost
Reinforcement Learning	Q-Learning, DQN	Adaptive and self-improving	Complex to implement

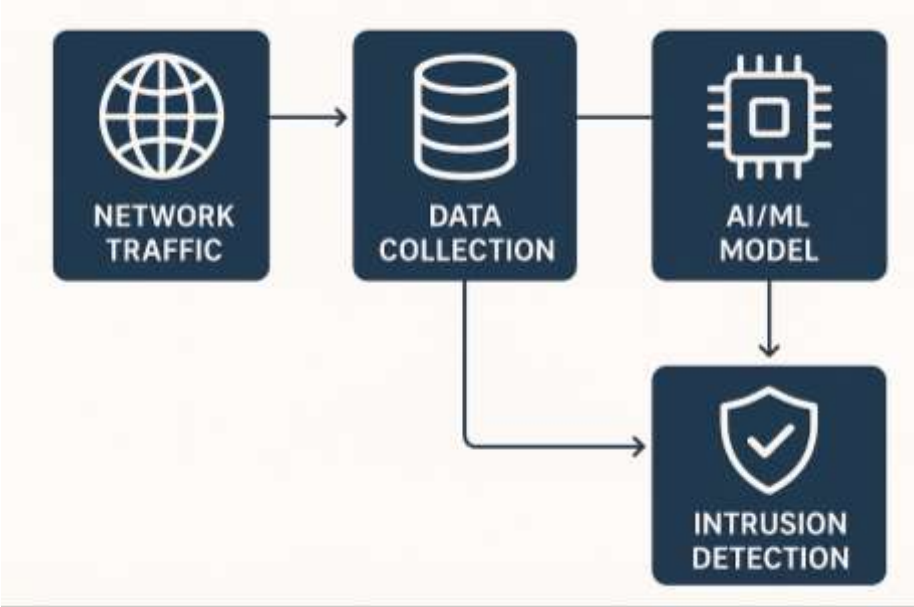

Figure 1: Architecture of an AI/ML-Driven Intrusion Detection System

Unsupervised Learning Approaches

In scenarios where labeled data is unavailable, unsupervised learning algorithms like K-Means Clustering, DBSCAN, and Autoencoders are employed. These models detect anomalies by identifying deviations from established behavioral patterns, making them useful for identifying zero-day attacks.

Deep Learning Architectures

Deep learning enables automatic feature extraction from high-dimensional data. CNNs analyze spatial traffic patterns, while LSTMs capture temporal dependencies in sequential network data. Deep Autoencoders can detect complex anomalies by reconstructing input data and measuring reconstruction errors. These models outperform traditional ML algorithms in large-scale network environments.

Reinforcement Learning for Adaptive Defense

Reinforcement Learning (RL) introduces a dynamic decision-making capability to IDS. By interacting with network environments, RL agents learn optimal defense strategies that minimize risk. Such systems evolve with the threat landscape, providing proactive protection rather than reactive responses.

THREAT PREDICTION USING AI AND ML

The growing sophistication of cyber threats has highlighted the need for predictive cybersecurity solutions that not only detect attacks but also anticipate them before they cause damage. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as essential tools in this domain, enabling proactive defense strategies that reduce risk exposure and improve system resilience. Threat prediction involves analyzing historical and real-time data to forecast potential security incidents, attack vectors, and system vulnerabilities.

PREDICTIVE ANALYTICS IN CYBERSECURITY

Predictive analytics applies statistical and machine learning techniques to identify patterns and trends in historical data that may indicate future threats. In cybersecurity, predictive models leverage time-series data, behavioral analytics, and contextual intelligence to detect early warning signals of potential attacks.

- **Time-Series Analysis:** By analyzing sequential network traffic, login patterns, or transaction logs over time, AI models can identify unusual spikes or deviations indicative of malicious activity. For example, a sudden surge in failed login attempts or abnormal data transfer rates may signal an impending brute-force or data exfiltration attack.

- **Behavioral Analysis:** Machine learning algorithms can learn normal patterns of user and device behavior, establishing a baseline. Any deviation from this baseline, such as access

at unusual hours or interaction with unexpected resources, can trigger alerts. Techniques such as clustering and anomaly detection are commonly used to model these behaviors.

- **Contextual Intelligence:** Predictive models also incorporate external factors such as threat intelligence reports, system configurations, and known vulnerabilities to enhance prediction accuracy. By integrating contextual information, AI/ML models can differentiate between benign anomalies and genuine threats, improving decision-making.

These predictive analytics capabilities allow security teams to identify vulnerabilities and respond to threats before they escalate, reducing the likelihood of significant breaches.

GRAPH-BASED AND TEMPORAL MODELS

Modern networks are highly interconnected, with complex relationships between users, devices, and applications. Graph-based and temporal models provide advanced mechanisms to understand and predict threats in such environments.

- **Graph Neural Networks (GNNs):** GNNs model relational data, such as user-device interactions, application dependencies, and network topologies. By representing a network as a graph where nodes are entities and edges are interactions, GNNs can detect subtle attack patterns like lateral movement in enterprise networks, privilege escalation chains, or coordinated botnet activities.

- **Temporal Models (LSTM, GRU):** Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) networks are capable of learning temporal dependencies in sequential data. These models are particularly effective for predicting multi-stage or coordinated attacks that unfold over time. For example, an attacker may first gain low-level access, probe system resources, and then escalate privileges—temporal models can identify these sequential steps early.

- **Hybrid Approaches:** Combining graph-based and temporal modeling enables systems to capture both structural relationships and sequential attack dynamics, providing a more comprehensive predictive capability. This hybrid approach is particularly useful in complex enterprise or cloud environments where attacks may follow intricate paths.

INTEGRATION WITH THREAT INTELLIGENCE FEEDS

AI/ML-driven intrusion detection and threat prediction systems are often enhanced by integrating external threat intelligence feeds. These feeds provide Indicators of Compromise (IOCs), such as known malicious IP addresses, domains, malware signatures, and phishing URLs.

- **Correlation with Internal Data**: Machine learning models correlate these external indicators with internal system logs, network flows, and user activity to identify vulnerabilities and potential attack paths.
- **Real-Time Threat Assessment**: AI can continuously ingest and analyze these feeds, updating the predictive models in near real-time to anticipate emerging threats.
- **Use Cases**: For instance, if a threat intelligence feed reports a new ransomware campaign targeting certain file types, the AI system can predict which internal systems are likely to be affected based on file access patterns, user privileges, and network topology.

This integration transforms traditional IDS from a reactive monitoring tool into a proactive threat prediction engine, capable of mitigating attacks before they manifest.

SIMULATION AND ATTACK FORECASTING

Simulation-based threat prediction uses AI/ML techniques to model potential attack scenarios and forecast their impact on the network.

- **Reinforcement Learning for Scenario Simulation:** Reinforcement learning agents can simulate attacker behavior, exploring possible attack paths and estimating the probability of success for various threats. By iteratively learning from these simulations, the system identifies critical vulnerabilities and recommends preventive measures.

- **Adversarial Modeling:** Generative Adversarial Networks (GANs) and similar adversarial approaches can simulate sophisticated attacks that mimic real-world strategies, testing the robustness of predictive models. This allows organizations to strengthen their defenses against previously unseen attack types.
- **Proactive Defense Planning**: Forecasting models enable security teams to allocate resources efficiently, prioritize patching of vulnerable systems, and implement dynamic access controls before an attack occurs. For example, AI could predict that certain user

accounts or network segments are at higher risk and enforce multi-factor authentication or traffic monitoring preemptively.

Simulation and attack forecasting not only predict threats but also support strategic cybersecurity planning, making it possible to minimize risk exposure and ensure rapid response in high-stakes environments.

CHALLENGES IN AI/ML-BASED INTRUSION DETECTION

Table 3: Common Datasets Used for AI-Based Intrusion Detection Research

Dataset Name	Year	Type of Data	Remarks
KDD Cup 99	1999	Network traffic (TCP/IP)	Widely used but outdated
NSL-KDD	2009	Improved version of KDD	Balanced dataset
CICIDS2017	2017	Modern network traffic with latest attacks	Realistic and comprehensive
UNSW-NB15	2015	Hybrid normal and malicious data	Used for benchmarking ML models
TON_IoT	2020	IoT and IIoT telemetry	Relevant for edge/IoT security

Data Quality and Imbalance

Intrusion detection datasets often contain class imbalances, where normal traffic heavily outweighs malicious samples. This imbalance leads to biased learning and reduced detection of rare attack types. Generating synthetic attack data or using data augmentation techniques can partially address this issue.

Adversarial Attacks on ML Models

AI-based IDS themselves can be targets of adversarial manipulation. Attackers can craft subtle perturbations in network data to evade detection, leading to model misclassification. Robust adversarial training and model hardening are crucial countermeasures.

Explainability and Transparency

Black-box nature of deep learning models poses interpretability challenges. Security analysts need to understand the reasoning behind a model's decisions, especially for critical defense operations. Research in Explainable AI (XAI) aims to make these systems more transparent and trustworthy.

Computational Overhead and Real-Time Processing

AI models, particularly deep networks, require significant computational resources. Implementing them in real-time intrusion detection systems demands optimization, hardware acceleration, and efficient inference techniques.

Privacy and Ethical Concerns

Collecting and analyzing user data for security purposes raises privacy issues. Developing privacy-preserving ML models that maintain confidentiality while ensuring accurate threat detection remains a significant challenge.

APPLICATIONS OF AI/ML-BASED IDS

Network Traffic Analysis

AI models analyze vast volumes of network traffic to identify malicious activity, such as Distributed Denial-of-Service (DDoS) attacks or data exfiltration attempts.

Cloud Security and Virtualization Environments

Machine learning enhances cloud-based IDS by adapting to dynamic workloads and virtual machine migrations, ensuring security in multi-tenant environments.

IoT and Edge Security

AI-based IDS are crucial in IoT ecosystems where devices have limited computational power and are prone to diverse attacks. Lightweight ML models enable localized threat detection at the edge level.

Industrial Control Systems (ICS)

AI-driven intrusion detection safeguards critical infrastructure, such as power grids and manufacturing systems, by monitoring operational parameters and detecting deviations

indicative of cyber sabotage.

SCOPE AND FUTURE PROSPECTS

Integration with Zero-Trust Architectures

AI/ML-based IDS can enhance zero-trust frameworks by continuously validating user and device trust levels. This integration ensures that no entity within the network is implicitly trusted.

Autonomous Cyber Defense Systems

The next generation of cybersecurity solutions will feature self-healing and self-learning capabilities. By combining AI with automation and orchestration platforms, networks can autonomously detect, respond, and recover from attacks.

Federated Learning for Privacy Preservation

Federated Learning allows collaborative model training without sharing sensitive data across organizations, thus ensuring privacy while improving detection accuracy.

Quantum-Resilient Threat Detection

As quantum computing evolves, AI/ML-based models must adapt to detect quantum-enabled attacks. Hybrid quantum-classical AI systems may become integral to future cyber defense mechanisms.

Real-Time Threat Intelligence and Visualization

Future systems will emphasize real-time threat visualization dashboards powered by AI analytics, allowing security teams to interpret risks intuitively and respond effectively.

CONCLUSION

AI and ML are redefining the boundaries of cybersecurity by transforming traditional intrusion detection systems into intelligent, predictive, and adaptive defense mechanisms. Through advanced analytics, deep learning, and real-time threat modeling, AI/ML-driven IDS can detect, classify, and predict complex cyberattacks that traditional methods often miss. Despite challenges such as data imbalance, adversarial manipulation, and lack of explainability, continued research and innovation promise a more secure digital future. The integration of

AI/ML in cybersecurity not only strengthens network resilience but also paves the way toward fully autonomous and proactive cyber defense ecosystems, essential for safeguarding next-generation digital infrastructures.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*(1), 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
2. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset for Internet of Things (IoT) and Industrial IoT (IIoT) cybersecurity research. *IEEE Access, 8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022864
3. 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. https://doi.org/10.1109/COMST.2015.2494502
4. Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *ACM Computing Surveys, 51*(3), 1–36. https://doi.org/10.1145/3241738
5. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2019). Intelligent anomaly-based intrusion detection for cloud environments using machine learning. *Computers & Security, 87*, 101640. https://doi.org/10.1016/j.cose.2019.101640
6. Choudhary, S., & Nagar, R. (2021). AI and machine learning-based network intrusion detection systems: A review. *International Journal of Information Security Science, 10*(2), 56–70.
7. Ding, S., & Zou, D. (2021). Deep reinforcement learning for adaptive cyber defense: A review. *IEEE Access, 9*, 145432–145449. https://doi.org/10.1109/ACCESS.2021.3119588
8. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003
9. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., & Tachtatzis, C. (2017). Threat analysis of IoT networks using artificial neural network intrusion detection system. *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6. https://doi.org/10.1109/ISNCC.2016.7746067

10. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (BICT)*, 21–26. https://doi.org/10.4108/eai.3-12-2015.2262516