International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

AI-based Cyber Threat Prediction Framework for Enterprise Security

Mohit Japee [1] , Parthi Soni [2]
[1] Student, Computer Studies and Emerging Technology, TransStadia University, Ahmedabad
Email: mohitjapee@gmail.com
[2] Assistant Professor, School of Computer Studies and Emerging Technology, TransStadia University, Ahmedabad
Email: parthisoni7396@gmail.com

Abstract- Modern enterprise networks generate a large volume of security events, making it difficult for security analysts to identify critical threats in real time. Traditional rule-based detection mechanisms often fail to detect advanced and evolving cyber attacks. Artificial Intelligence (AI) and Machine Learning (ML) techniques have shown promising capabilities in analyzing large-scale security data and predicting potential cyber threats. This research proposes an AI-based cyber threat prediction framework designed to enhance threat detection and decision-making in enterprise environments. The framework focuses on log analysis, anomaly detection, and threat prediction using machine learning techniques. The study highlights the potential of predictive analytics in improving proactive cybersecurity strategies and reducing response time in security operations centers (SOCs). The proposed framework is conceptual and aims to provide a cost-effective and scalable approach for organizations adopting intelligent cybersecurity solutions.

Keywords: Cybersecurity, Threat Prediction, Attack Forecasting, AI, Machine Learning, Incident Response Automation, SOC, SIEM, SOAR, Enterprise Security.

I. INTRODUCTION

The importance of cybersecurity as an operational need for organizations cannot be overstated because of the fast expansion of digital systems, cloud computing, remote working arrangements, and online business. The attackers in the modern age are highly proficient and automated. The process of contemporary cyberattacks includes reconnaissance, gaining entry, obtaining elevated privileges, moving laterally across the network, establishing persistence, and stealing sensitive information.

However, most businesses continue to rely on conventional cybersecurity tools such as firewalls, anti-virus programs, and intrusion detection systems based on signatures. Such tools are effective but fail to deal with threats that have not been encountered before and sophisticated persistent attacks. SOC departments receive numerous alerts every day and experience alert fatigue. There are many attacks that go unnoticed due to the fact that they fall into a noisy environment.
AI and ML techniques can be used effectively to analyze massive security logs, discover anomalies, and predict the future stages of an attack. Another important aspect of cyber defense is automated response because manually performing this task takes too much time and does not provide consistent results. The proposed research focuses on developing a unified system based on AI for threat prediction and automated decision-support, addressing the limitations of existing reactive security measures.

II. RELATED WORK AND LITERATURE REVIEW

A substantial body of research concerning AI in cybersecurity has emerged recently, specifically concerning intrusion detection, anomaly detection, and threat intelligence. Buczak and Guven provide a comprehensive survey on using machine learning methods for cyber security intrusion detection, demonstrating how ML algorithms can surpass the effectiveness of signature-based techniques in response to constantly changing attacks [1]. Ring et al. summarize existing machine learning applications for network intrusion detection, describing common datasets, assessment techniques, and potential problems related to data imbalance [2]. Furthermore,

studies by Sommer and Paxson underscore the challenge of applying machine learning outside a closed-world assumption for network intrusion detection [4], while Shone et al. demonstrate the effectiveness of deep learning approaches in complex traffic environments [5]. Although detection remains one of the most studied issues, researchers also pay increasing attention to cyber threat prediction. Predictive systems often apply time-series models, machine learning techniques, and attack graphs, such as those derived from the MITRE ATT&CK framework [6], to analyze past activities and forecast future attack steps. The UNSW-NB15 dataset is a notable resource for network intrusion detection research [3]. In response, Security Orchestration, Automation, and Response (SOAR) have gained widespread attention. However, the literature discusses difficulties associated with response automation, such as false alarms and the necessity for human validation, suggesting a need for decision-support mechanisms rather than fully automated actions. From the literature review, significant contributions exist in detection, but prediction and response automation require further integrated research.

III. MOTIVATION AND PROBLEM FORMULATION

Organizations face significant challenges in managing cyber threats due to increasing attack complexity and large volumes of security alerts. Existing systems primarily focus on detection rather than prediction, resulting in delayed responses to cyber incidents. Key challenges include:

- High volume of alerts causing alert fatigue
- Limited predictive capabilities in traditional security tools
- Slow manual incident response processes
- Difficulty in prioritizing critical threats
- Lack of intelligent decision-support mechanisms.

Therefore, there is a need for an intelligent framework that can analyze security data and predict potential threats before they escalate into major incidents.

IV. PROPOSED FRAMEWORK AND METHODOLOGY

The proposed framework is a conceptual security system that involves the use of AI in predicting and responding to attacks. The proposed system has five layers:

Data Collection Layer
This layer collects events from various sources:

- Network IDS (Suricata)
- Firewall logs
- Authentication logs (Windows/Linux)
- Web server logs
- Optional Endpoint Telemetry

Pre-processing and Feature Engineering Layer
This layer converts logs to a normalized data format including:

- Timestamps
- IP, Ports, Protocols
- User activity features
- Frequency and sessions features

Detection Layer (AI)
This layer will detect:

- Network anomalies
- Suspicious logins
- Anomalous traffic
- Known intrusions with ML-based detection

Threat Prediction Layer
This novel layer performs predictions by detecting:

- Probability of attack escalation
- Next-step predictions
- Lateral movement/privilege escalation risks

These predictions can be made using:

- Time Series prediction using LSTMs
- Sequence modeling using transformer-based models
- MITRE ATT&CK attack graphs

Decision-Support and Response Layer
This layer provides decision-support recommendations to assist security analysts in responding to predicted threats.

The response component focuses on generating alerts and recommended actions based on predicted threats, instead of performing fully automated actions. Typical recommended actions include: blocking IP addresses, limiting traffic rate, taking down hijacked accounts, isolating endpoints, and generating incident reports for SOC analysis.

Technical Implementation Stack
Suricata: Network Intrusion Detection System and alerts
Python: Data processing and ML integration
Flask/FastAPI: Backend API services

Libraries: Scikit-learn, TensorFlow, PyTorch
Databases: PostgreSQL/SQLite
Dashboard: Web-based SOC interface

V. RESULTS, DISCUSSION, AND FUTURE SCOPE

Expected Impact and Benefits

- Increased Early Detection: AI-based systems enhance detection of abnormalities compared to static rules.
- Threat Prioritization: Scoring helps SOC analysts focus on high-priority incidents.
- Pre-emptive Defense: Prediction enables mitigation before attacks reach advanced stages.
- Operational Efficiency: Automation reduces response times from hours to minutes.

Challenges and Limitations

- Data Quality: Models require high-quality historical data for effective training.
- False Positives: Incorrect automated responses can disrupt business continuity.
- Model Drift: Continuous retraining is necessary as attack patterns evolve.

Future Work

- The use of Explainable AI (XAI) for SOC trust
- The implementation of Graph Neural Networks (GNN) for attack chains prediction
- SOAR systems for full integration

VI. CONCLUSION

This study presents a conceptual framework for AI-based cyber threat prediction in enterprise environments. The proposed model demonstrates how machine learning techniques can support proactive cybersecurity strategies by analyzing security data and identifying potential threats. Future work may involve implementing and evaluating the framework using real-world datasets to validate its effectiveness in practical security environments

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. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). 'A Survey of Network-Based Intrusion Detection Data Sets.' Computers & Security, 86, 147–167.
3. A.Moustafa, N., & Slay, J. 'The UNSW-NB15 Dataset for Network Intrusion Detection Systems.'
4. Sommer, R., & Paxson, V. (2010). 'Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.' IEEE Symposium on Security and Privacy.
5. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). 'A Deep Learning Approach to Network Intrusion Detection.' IEEE Transactions on Emerging Topics in Computational Intelligence.
6. MITRE Corporation. MITRE ATT&CK Framework. https://attack.mitre.org