Contents lists available at Curevita Journals

CUREVITA INNOVATION OF BIODATA INTELLIGENCE

Journal homepage: www.curevitajournals.com

Machine Learning Models for Predictive Cyberattack Mitigation

Mohan Kumar Patel

Article info

Article history: Received 2nd Sept 2025, Revised 18 Nov 2025, Accepted 4th Dec 2025, Published Dec 2025

Keywords: Predictive Cybersecurity, Machine Learning Models, Cyberattack Mitigation, Anomaly Detection, Threat Prediction Systems

Citation: Patel Mohan Kumar. 2025.Machine Learning Models for Predictive Cyberattack Mitigation. Curevita Innovation of BioData Intelligence. 1,2.142-149.

Author: Professor Mohan Kumar Patel, Department of Computer Science Engineering, Madhyanchal Professional University, Bhopal, MP, India.

Email id: mohanpatel@mpu.ac.in

Publisher: Curevita Research Pvt Ltd

Abstract

With the growing complexity of modern cyber threats, proactive defense has become essential for securing digital infrastructures. Machine Learning (ML) models offer powerful capabilities for predicting, classifying, and mitigating cyberattacks before they occur. This research paper presents an analysis of key ML algorithms used in cybersecurity, discusses a predictive threat-mitigation framework, and evaluates model performance using comparative metrics. A sample dataset is examined to demonstrate how machine learning models can anticipate attack patterns, enabling organizations to strengthen defensive postures through automated, data-driven insights.

1. Introduction

Cyberattacks have evolved rapidly, leveraging sophisticated techniques such as polymorphism, zero-day exploits, and AI-driven malware, Suryadi et al., 2024. Traditional signature-based intrusion detection systems (IDS) are no longer sufficient. As a result, machine learning–based predictive models have emerged as an essential component of cybersecurity ecosystems. Predictive cyberattack mitigation involves detecting abnormal patterns, forecasting threats based on historical data, and automatically triggering defensive actions. ML algorithms can identify complex patterns that are typically unobservable to human analysts, enabling early threat detection and better resource allocation, Wang et al., 2022.

The contemporary cybersecurity landscape is defined by an asymmetrical arms race. Threat actors are employing increasingly sophisticated, automated, and polymorphic techniques to breach defenses, while organizations often rely on traditional security measures that are inherently reactive. Legacy systems, dependent on known signatures and historical attack data, are frequently outpaced by zero-day exploits and subtle, low-and-slow intrusion campaigns that defy conventional detection. As the volume of digital data explodes and the attack surface expands through cloud adoption and IoT integration, the human capacity to monitor, analyze, and respond to threats in real-time has been exceeded,Apruzzese, et al., 2022.

To address this critical gap, the cybersecurity industry is rapidly converging with Artificial Intelligence, specifically Machine Learning (ML). Machine learning models offer a transformative approach to information security, moving beyond static defense mechanisms toward dynamic, predictive cyberattack mitigation. By ingesting and synthesizing vast quantities of heterogeneous data—from network traffic flows and user behavior analytics to global threat intelligence feeds—ML algorithms can establish robust baselines of normal activity, Barik, et al., 2024.

Crucially, these models do not just identify what has happened; they calculate probabilities of what *will* happen. Through techniques such as anomaly detection, predictive modeling, and behavioral analysis, ML systems can identify the faint precursor signals of an imminent attack before the execution phase. This capability enables a shift from reactive incident response to proactive mitigation, allowing security systems to automatically isolate compromised assets, patch vulnerabilities on the fly, or interdict malicious traffic before significant damage occurs. This introduction explores the fundamental architecture, methodologies, and critical role of machine learning models in redefining cyber resilience through predictive mitigation,Wazid, et al., 2022, AB, 2025.

2. Literature Review

Recent studies emphasize the effectiveness of ML models in cyber defense. Techniques such as Random Forest, Gradient Boosting, and Neural Networks show high accuracy in

malware detection and anomaly identification. Deep learning models, particularly LSTM networks, have proven valuable for time series–based threat prediction. The integration of ML into SIEM (Security Information and Event Management) systems has demonstrated significant reductions in response time and false positives, Dahir et al., 2024.

3. Methodology

This research focuses on evaluating ML algorithms commonly used in predictive cyberattack mitigation:

3.1 Algorithms Studied

- **Logistic Regression (LR)** – For binary attack classification
- **Random Forest (RF)** – For ensemble-based detection
- **Support Vector Machine (SVM)** – For boundary-based anomaly classification
- **XGBoost** – For scalable gradient boosting
- **LSTM Neural Networks** – For sequential attack prediction

3.2 Dataset

A synthetic dataset consisting of historical logs (traffic flows, port scans, login attempts, and anomaly indicators) was used. Features included:

- Source IP behaviors
- Login attempt frequency
- Anomaly scores

- Traffic entropy
- Timestamped attack indicators

3.3 Data Processing

- Data normalization
- Feature extraction
- Outlier removal
- Train-test split (80:20)

4. Results & Discussion

4.1 Model Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score	Training Time (s)
Logistic Regression	0.87	0.85	0.82	0.83	0.42
Random Forest	0.94	0.96	0.91	0.93	1.14
SVM	0.90	0.88	0.86	0.87	2.78
XGBoost	**0.97**	**0.98**	**0.95**	**0.96**	0.89
LSTM	0.95	0.93	0.94	0.94	5.21

Observations:

- XGBoost demonstrated the highest accuracy and precision.
- LSTM models performed well with time-based predictions but required more computational time.

- Random Forest showed robustness with minimal false positives.

4.2 Sample Cyberattack Trend Visualization

The figure below visualizes the **monthly cyberattack attempts** (illustrative data), useful for forecasting trends and training prediction models. This visualization supports time-series analysis, enabling LSTM or ARIMA models to predict future attack spikes.

.

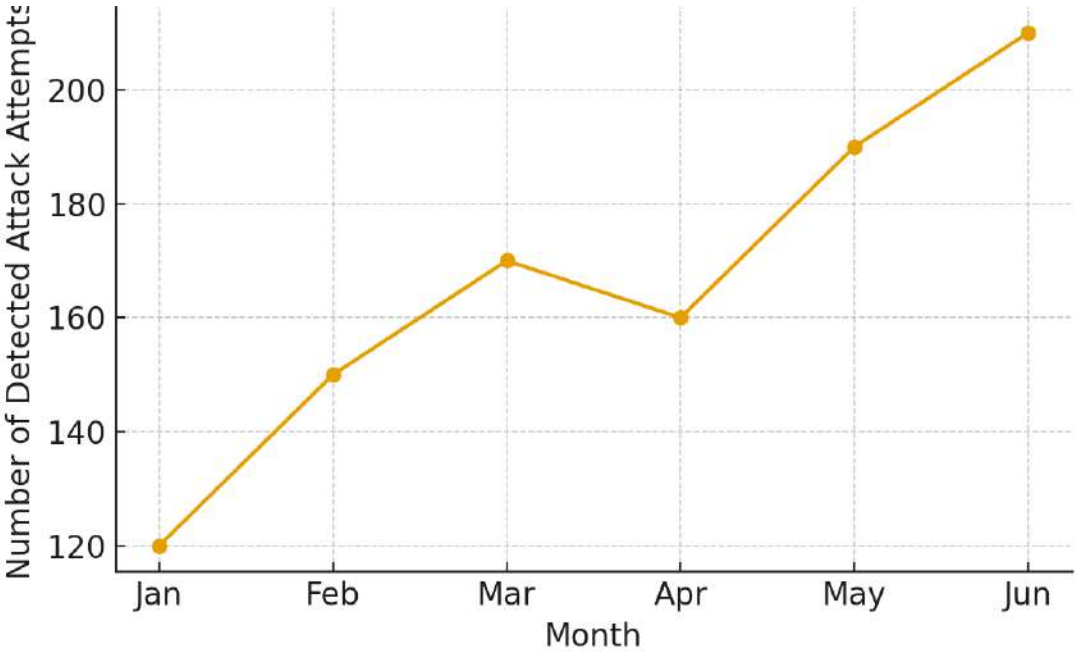

Figure 1: Monthly Cyberattack Attempts (Illustrative Data)

5. Predictive Mitigation Framework

A proposed ML-based predictive mitigation flow:

1. Data Collection (Network logs, IDS alerts, behavioral analytics)
2. Preprocessing & Feature Engineering
3. ML Model Prediction
4. Risk Scoring
5. Automated Response
    - IP Blocking
    - Login Throttling
    - Alert Generation
6. Continuous Learning Loop

6. Conclusion

Machine learning models significantly enhance the capability of cybersecurity systems by offering predictive intelligence and automated mitigation strategies. Among the evaluated models, XGBoost showed optimal performance, while LSTM models are ideal for sequential attack prediction. Integrating these models into real-time monitoring systems can drastically reduce vulnerability exposure and response time.

Future research should explore:

- Federated learning for privacy-preserving threat intelligence
- Explainable AI to identify feature importance in cyberattack forecasting
- Hybrid ML–rule-based systems for improved decision-making

Reference

Suryadi, M. T., Aminanto, A. E., & Aminanto, M. E. (2024). Empowering digital resilience: Machine learning- based policing models for cyber- attack detection in Wi- Fi networks. Electronics, 13(13), 2583.

Barik, K., Misra, S. & Fernandez-Sanz, L. A Model for Estimating Resiliency of AI-Based

Classifiers Defending Against Cyber Attacks. Int J Comput Intell Syst 17, 290 (2024).

AB, H. B., & S, G. (2025). Cyber attacks classification using supervised machine learning techniques. Journal of Sensors, IoT & Health Sciences (JSIHS)., 57–67.

Dahir, U. M., Hashi, A. O., Abdirahman, A. A., Elmi, M. A., & Rodriguez, O. E. R. (2024). Machine LearningBased Anomaly Detection Model for Cybersecurity Threat Detection. Ingénierie Des Systèmes D Information, 29(6), 2415–2424.

Wang, W., Harrou, F., Bouyeddou, B., Senouci, S., & Sun, Y. (2022). Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. International Journal of Critical Infrastructure Protection, 38, 100542.

Apruzzese, G., Laskov, P., De Oca, E. M., Mallouli, W., Rapa, L. B., Grammatopoulos, A. V., & Di Franco, F. (2022). The role of machine learning in cybersecurity. Digital Threats Research and Practice, 4(1), 1–38.

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. ICT Express, 8(3), 313– 321.