Int Journal of Engineering and Computer Science

Open access

Commentary

Machine Learning Algorithms for Cyber Threat Detection

Ahmed Hassan*

**Center for Data Science and Analytics, Future Research University, Dubai, UAE*

***Correspondence:** Ahmed Hassan, Center for Data Science and Analytics, Future Research University, Dubai, UAE, E-mail: emiliy1988@gmail,com; DOI: 10.1042/JCTCS.4.1.0007

Received date: Apr 02, 2026; **Accepted date:** Apr 12, 2026; **Published date:** Apr 30, 2026

Citation: Ahmed Hassan (2026) Machine Learning Algorithms for Cyber Threat Detection. Int J Eng Comp Sci. 4: 1.

Introduction

Machine learning algorithms are generally classified into supervised, unsupervised, semi-supervised, and reinforcement learning methods.

Supervised learning

Supervised learning algorithms use labeled training datasets to classify network traffic or executable files as either benign or malicious. Common algorithms include:

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- Logistic Regression
- Naïve Bayes
- Gradient Boosting

These techniques are widely used in malware classification and intrusion detection because they provide strong predictive performance when high-quality labeled datasets are available.

Unsupervised learning

Unsupervised learning identifies abnormal patterns without requiring labeled datasets.

Common algorithms include:

- K-Means Clustering
- DBSCAN
- Isolation Forest
- Autoencoders
- Principal Component Analysis (PCA)

These methods are particularly useful for detecting unknown attacks and zero-day threats.

Reinforcement learning

Reinforcement learning enables cybersecurity agents to learn optimal defense strategies through interaction with dynamic environments.

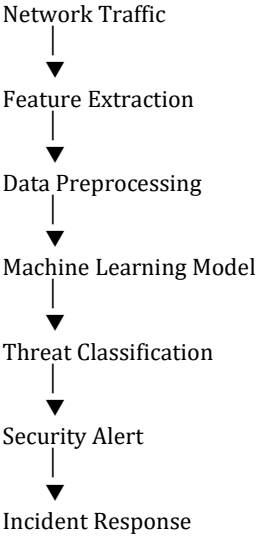
Applications include:

- Adaptive firewall configuration
- Dynamic access control
- Network defense optimization
- Autonomous incident response

Table 1: Machine learning algorithms used in cybersecurity.

Algorithm	Learning Type	Common Applications	Advantages	Limitations
Decision Tree	Supervised	Intrusion Detection	Easy interpretation	Overfitting
Random Forest	Supervised	Malware Detection	High accuracy	Increased computation
Support Vector Machine	Supervised	Spam Detection	Effective in high-dimensional data	Parameter tuning required
K-Means	Unsupervised	Anomaly Detection	Simple implementation	Sensitive to initialization
Isolation Forest	Unsupervised	Insider Threat Detection	Efficient anomaly detection	Limited explainability
Reinforcement Learning	Reinforcement	Adaptive Defense	Continuous learning	High training complexity

Figure 1: AI-Based cyber threat detection pipeline.



References

1) Zhao Y, Zhang X, Wei Y. Neuronal injuries in cerebral infarction and ischemic stroke: From mechanisms to treatment (Review). Int Mol Med. 2022, 49:15.
2) Feduto MA, Maksimovich N Ye, Bon EI, Zimatkin SM. Modeling of cerebral anoxia of respiratory genesis in rats. Arch Urol Nephrol. 2023, 2:1-4.
3) Feduto MA, Maksimovich N Ye, Bon EI, Zimatkin SM. Comparative characteristics of morphological changes in neurons of the parietal cortex of rats with anoxia of ischemic and respiratory genesis. Arch Repr Med. 2023, 1-4.
4) Feduto MA, Maksimovich N Ye, Bon EI, Zimatkin SM. Histological disorders of the neurons of the occipital cortex of the brain of rats with mechanical asphyxia in dynamics. News of Biomed Sci. 2022, 22:93-94.
5) Maksimovich NE, Bon E, Zimatkin SM. The rat brain and its response to ischemia: monograph. Grodno: GrGMU. 2020, 1:240.
6) Paxinos G. The rat brain in stereotaxis coordinates. Academic Press. 1998, 9: 242.
7) Maksimovich N Ye, Bon EI, Zimatkin SM. Central nervous system of the rat: textbook. GrSMU. 2022, 226.
8) Brown BM, Newcombe RG. Non-null semi-parametric inference for the Mann-Whitney measure. J Nonpar Stat. 2009, 743.