DEVELOPMENT OF A MACHINE LEARNING ALGORITHM FOR RISK ASSESSMENT IN INTERNET OF THINGS (IOT) SYSTEMS

Happy Ondobo Steve [1], Vitaly B. Kreindelin [2]

[1] University of Buea, Buea, Cameroon, happionodobo@gmail.com
[2] MTUCI, Moscow, Russia, vitkrend@gmail.com

ABSTRACT

Machine learning offers a promising approach to automating risk assessment by analyzing patterns in network traffic. This work builds upon existing anomaly and intrusion detection methods while addressing the lack of IoT-specific risk assessment frameworks that incorporate both the likelihood of occurrence and the impact of security incidents. The rapid expansion of the Internet of Things (IoT) has created significant challenges for ensuring the security and resilience of interconnected devices. Traditional security approaches are insufficient to protect against dynamic, evolving cyber threats. This paper proposes an IoT risk assessment framework based on machine learning, integrating both supervised and unsupervised techniques to identify, classify, and mitigate threats. The framework evaluates risks based on likelihood and impact, providing a scalable and adaptive solution suitable for modern IoT networks.

DOI: 10.36724/2664-066X-2026-12-4-32-38

Received: 05.04.2026
Accepted: 17.06.2026

Citation: Happy Ondobo Steve, Vitaly B. Kreindelin, "Development of a machine learning algorithm for risk assessment in Internet of Things (IoT) systems," *Synchroinfo Journal* **2026**, vol. 12, no. 4, pp. 32-38.

KEYWORDS: *IoT security, risk assessment, machine learning, anomaly detection, cybersecurity.*

Licensee IRIS, Vienna, Austria.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Copyright: © 2026 by the authors.

Introduction

The Internet of Things (IoT) connects billions of devices worldwide, transforming sectors such as healthcare, manufacturing, transportation, and smart cities. However, heterogeneity, limited computational power, and a lack of robust security protocols render IoT devices vulnerable to cyberattacks, as highlighted in the OWASP IoT Top Ten Security Threats [1].

Key challenges include the constrained resources of these devices, heterogeneous architectures, and inadequate security protocols. Such vulnerabilities expose IoT environments to risks including malware, denial-of-service attacks (e.g., the Mirai botnet [2]), data breaches, and advanced persistent threats.

Risk assessment is a critical step in securing the Internet of Things, as it enables system administrators to prioritize threats based on their severity. Traditional methods rely heavily on static rules [3]. Machine learning (ML) offers a promising approach to automating risk assessment by analyzing patterns within network traffic [4, 5].

This work builds upon existing anomaly and intrusion detection methods while addressing the current lack of IoT-specific risk assessment frameworks that incorporate both the likelihood of occurrence and the impact of security incidents [6].

Several studies have explored the integration of machine learning into IoT security. Signature-based detection methods are effective against known threats but fail to address unknown ones. Behavioral and anomaly-based detection methods improve detection capabilities, yet they are prone to a high rate of false positives [4]. Platforms such as Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Information and Event Management (SIEM) provide monitoring and detection, but – as noted by NIST – they lack configurations specifically tailored to IoT environments [7].

Recent research highlights the potential of machine learning algorithms, including Random Forest, Support Vector Machines, and Neural Networks, for detecting IoT anomalies. For instance, the N-BaIoT study demonstrated the effectiveness of deep autoencoders in identifying botnet attacks [5], while hybrid deep learning models have shown promise for intelligent threat detection [8]. Nevertheless, few studies focus specifically on risk assessment that incorporates both the probability of an attack and its potential impact on IoT systems [6]. Furthermore, emerging technologies like Federated Learning offer privacy-preserving solutions, enabling collaborative model training without the need to share raw data [9].

Statement of the problem

The purpose of this paper is to develop and evaluate an algorithm for risk assessment in IoT systems based on machine learning. The algorithm must be able to:

- Rel ably detect both known and previously unknown cyber threats.
- Reduce the number of false positives that can overwhelm system administrators.
- Create a meaningful risk assessment that combines the likelihood of an attack and its potential consequences.
- Efficiently scale to support large and complex IoT environments.

Addressing these issues will allow us to focus on the most serious risks, improve system resilience, and reduce the overall vulnerability of IoT ecosystems, consistent with the risk management goals of the NIST Cybersecurity Framework [10].

Let's consider the proposed methodology and algorithm development.

Methodology

The proposed framework operates in three stages: data preprocessing, threat detection, and risk assessment. Let us examine these stages in more detail (Fig. 1).

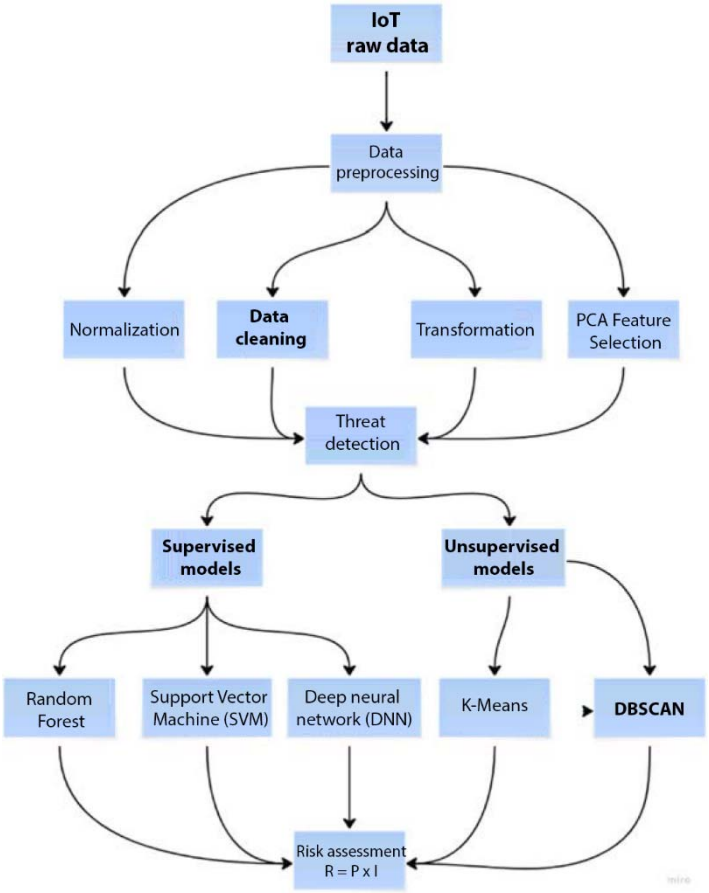


Fig. 1. Overall architecture of an IoT risk assessment system

1. Data Preprocessing: IoT traffic and device logs are normalized, cleaned, and transformed into structured features. Feature selection methods, such as Principal Component Analysis (PCA), are applied to reduce dimensionality. To ensure relevance, we will utilize datasets specifically designed for IoT security research, such as the IoT Network Intrusion Dataset [11].

2. Threat Detection: Both supervised and unsupervised models are deployed, following a hybrid approach outlined in recent research [8]. Supervised classifiers (Random Forest, Support Vector Machines, Deep Neural Networks) detect known threats using labeled datasets. Unsupervised clustering (K-Means, DBSCAN) identifies anomalies and emerging risks without prior labeling [5].

3. Risk Assessment (R = P × I) is calculated using specific metrics for both probability (P) and impact (I). This two-factor assessment enables system administrators to prioritize mitigation efforts – moving beyond simple detection toward actionable analysis, as advocated by industry leaders such as Palo Alto Networks Unit 42 [12].

• Probability (P): This represents the confidence level of our machine learning model's prediction, scaled from 0.0 to 1.0. For example, if a Random Forest classifier is 95% confident that an event is a DDoS attack, then P = 0.95.

• Impact (I): This is a predefined score (e.g., from 1 to 10) based on the type of threat and the criticality of the target device. For example:

– malw re on a smart light bulb: Low Impact (I = 2).

– data exfiltr tion from the health monitoring system: High impact (I = 9).

Calculation example

A brute-force attack attempt (P = 0.88) on a critical industrial control sensor (I = 10) would result in a risk score of R = 0.88 × 10 = 8.8 (high risk). The same attack on a non-critical environmental sensor (I = 3) would yield R = 0.88 × 3 = 2.64 (low risk). Such a detailed assessment enables administrators to effectively prioritize their responses.

Figure 1 illustrates the overall architecture of the IoT risk assessment system, while Figure 2 details the machine learning workflow. The system architecture is designed as follows:

1. Data Source Layer: Various IoT devices (sensors, actuators, cameras) generate raw network traffic and system logs.

2. Data Collection and Preprocessing Layer: A central gateway or cloud server collects the raw data, which is then normalized, cleaned, and structured for analysis.

3. ML Core Engine: The preprocessed data is fed into a hybrid machine learning model (combining supervised and unsupervised algorithms) to detect threats and calculate the probability (P).

4. Risk and Decision-Making Layer: The output from the machine learning engine is combined with impact metrics (I) from the device registry to calculate the final risk score (R = P × I).

5. Action and Visualization Layer: Prioritized risks and automated mitigation actions (e.g., isolating a device or blocking an IP address) are presented to administrators via a security dashboard for final decision-making.

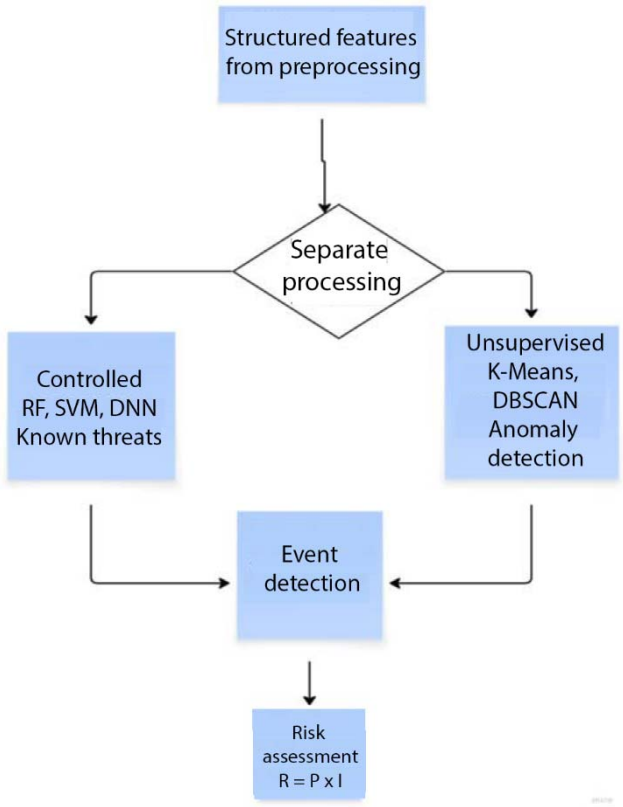


Fig. 2. Workflow of a machine learning algorithm

The IoT risk assessment algorithm is described as follows:

1. Input of pre-pr essed IoT data.

2. Applicati of feature selection for dimensionality reduction.

3. Training of supervised machine learning models using labeled datasets (e.g., NSL-KDD, CICIDS).

4. Execution of un pervised clustering to identify new risks.

5. Generation of a r k score for each event.

6. Provision of recommendations (e.g., isolating a device, enforcing encryption, or activating firewall rules).

Dataset and experimental design

Benchmark datasets for IoT and cybersecurity will be used for evaluation:

• NS -KDD – an intrusion detection dataset containing 125,000 records.

• CIC DS2017 – realistic traffic data including IoT botnet attacks (>3 million records).

• IoT-23 – a specialized dataset for IoT-related malware [11]. Table 1 presents the datasets and their characteristics.

Table 1

Datasets

Dataset	Description	Size
NSL-KDD	Dataset for classical intrusion detection	125,000 records
CICIDS2017	Realistic IoT traffic with botnet attacks	3M+ records
Internet of Things-23	Dedicated dataset on IoT malware traffic	20+ large pcap files

Expected results

Expected performance metrics are shown in Table 2. Deep neural networks are expected to outperform traditional machine learning methods, achieving an accuracy of up to 95%, which is consistent with the findings of Pajouh et al. [8].

Random Forest offers a balance between accuracy and interpretability, while unsupervised methods provide the additional capability to detect new, previously unseen threats. Table 2 presents the accuracy, precision/recall, and F1-score metrics for the models evaluated.

Table 2

Model metrics

Model	Accuracy	Memory Accuracy/Completeness	F1 account
Random forest	93%	91% / 90%	92%
Support Vector Machine	89%	88% / 87%	88%
Deep neural network	95%	94% / 93%	94%
K-means (unsupervised)	-	Detection level 70%	-

Our expected results indicate that a hybrid approach outperforms the use of a single model. The high accuracy of a deep neural network in identifying known threats, combined with the novel threat-detection capability of K-Means, creates a robust, layered defense.

• Comparison with related work: Unlike traditional SIEM systems, which rely on static rules [3], our framework dynamically adapts to new data. Furthermore, while many existing machine learning solutions focus solely on detection [5], our integration of impact-based risk assessment provides a direct, actionable output for system operators, addressing a key challenge in IoT security management [5, 12-15].

• Interpretation of unsupervised results: A lower detection rate (70%) is expected for the unsupervised model, as anomaly detection is inherently a complex task. Its value lies not in perfect accuracy, but in its ability to flag previously unknown attack patterns that supervised models might overlook, thereby providing an essential early-warning system.

Conclusion

This paper presents a comprehensive machine learning-based platform for assessing risks in the Internet of Things (IoT). By combining supervised and unsupervised learning methods, the framework is capable of detecting both known and novel threats while providing actionable risk assessments. The system emphasizes scalability and adaptability – qualities that are crucial in the rapidly evolving IoT landscape.

As part of our future work, we plan to:

• Deploy and test the system on a physical testbed consisting of actual IoT devices.

• Implement federated learning techniques [12] to train models across distributed devices without centralizing sensitive data.

• Develop a user-friendly dashboard that visualizes risk assessments and provides explanations for security teams.

REFERENCES

[1] OWASP Foundation. IoT Top Ten Security Threats. 2018.

[2] R. Sommer, V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” In *2010 IEEE Symposium on Security and Privacy*. 2010.

[3] D. Smith, et al., “Cybersecurity Challenges in IoT: A Risk-B ased Approach,” *Journal of Cybersecurity*. 2023.

[4] A. Dow, “Machine Learning for IoT Security: Techniques and Applications,” *IEEE Transactions on IoT*. 2022.

[5] Y. Meidan, M. Bohadana, Y. Mathov, et al., “N-BaIoT – Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” *IEEE Pervasive Computing*. 2018. https://ieeexplore.ieee.org/document/8324144.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, “A Multidimensional Robust and Adaptive Framework for IoT Risk Assessment,” *Computer Communications*. 2020. https://www.sciencedirect.com/science/article/abs/pii/S0140366419318341

[7] National Institute of Standards and Technology (NIST). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228). 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

[8] H. H. Pajouh, R. Javidan, R. Khayami, et al., “A Hybrid Deep Learning Model for Intelligent Threat Detection in IoT Systems,” *IEEE Access*. 2022. https://ieeexplore.ieee.org/document/9743117

[9] N. T. Nguyen, D. T. Hoang, D. N. Nguyen, et al., Federated Learning for IoT Security: A Case Study on Botnet Attack Detection,” *IEEE Transactions on Industrial Informatics*. 2023. https://ieeexplore.ieee.org/abstract/document/10020347

[10] National Institute of Standards and Technology (NIST). Cybersecurity Framework (Version 1.1). 2018.

[11] A. Alsaeedi, M. M. Rizvi, K. A. Al-Shqeer, “IoT Network Intrusion Dataset,” *MDPI Data*, 2019, no. 4(4), 141. https://www.mdpi.com/2306-5729/4/4/141

[12] Palo Alto Networks (Unit 42), The Role of AI and ML in IoT Security. 2023. https://unit42.paloaltonetworks.com/ai-machine-learning-iot-security/

13. V. B. Kreindelin, N. A. Legkov, “Protection of Authentication Data for Websites and Web Applications,” *Telecommunications and Information Technologies*. 2022. Vol. 9, No. 1, pp. 6-10.

[14] V. B. Kreindelin, A. D. Avidzba, “Encryption wi-fi protected access,” Technologies of the information society: XI International Industry Scientific and Technical Conference: collection of proceedings, Moscow, March 15-16, 2017. Moscow: Media Publisher, 2017. P. 294.

[15] V. B. Kreindelin, G. A. Vakhromeev, “Most Effective Machine Learning Algorithms for Risk-Based Authentication Systems,” *Telecommunications and Information Technologies*. 2024. Vol. 11, No. 1, pp. 87-92.