A Lightweight Machine Learning–Based Intrusion Detection System for Resource-Constrained IoT Networks

Author

Abhijeet Kumar Sriwastawa
Master of Computer Applications (MCA)
Email: meabhi14@gmail.com

Abstract

The rapid expansion of Internet of Things (IoT) devices in smart environments has significantly increased the vulnerability of network infrastructures to cyberattacks. Due to limited computational power, memory, and energy constraints, traditional security mechanisms are unsuitable for IoT ecosystems. Intrusion Detection Systems (IDS) based on conventional techniques often incur high computational overhead and fail to provide real-time protection. This paper proposes a lightweight machine learning–based intrusion detection framework specifically designed for resource-constrained IoT networks. The proposed approach integrates efficient feature selection techniques with lightweight machine learning classifiers to achieve high detection accuracy while minimizing computational complexity. Experiments conducted using the UNSW-NB15 dataset demonstrate that the proposed framework outperforms traditional IDS approaches in terms of accuracy, detection time, and false positive rate, making it suitable for real-time IoT security applications.

Keywords

Internet of Things; Intrusion Detection System; Machine Learning; Network Security; Lightweight Security

1 Introduction

The Internet of Things (IoT) paradigm enables seamless interconnection of heterogeneous devices such as sensors, actuators, and embedded systems, facilitating intelligent services in domains including healthcare, smart cities, industrial automation, and smart campuses. Despite its rapid adoption, IoT ecosystems remain highly vulnerable to cyber threats due to inherent constraints such as limited processing power, memory capacity, and energy availability.

Conventional security mechanisms such as firewalls and signature-based intrusion detection systems are insufficient for IoT environments, as they fail to detect zero-day attacks and require frequent updates. Machine learning–based intrusion detection systems have emerged as effective solutions capable of identifying complex attack patterns. However, many existing ML-based approaches rely on computationally expensive models that are unsuitable for deployment in resource-constrained IoT networks.

Moreover, existing research primarily focuses on maximizing detection accuracy without adequately addressing computational efficiency, latency, and scalability—critical requirements for real-time IoT security. This highlights the need for lightweight and efficient intrusion detection frameworks tailored to IoT environments.

This paper addresses these challenges by proposing a lightweight machine learning–based intrusion detection system optimized through feature selection techniques. The proposed framework aims to balance detection accuracy and computational efficiency, ensuring suitability for real-time IoT deployments.

2 Related Work

Several studies have investigated machine learning techniques for intrusion detection in IoT and networked environments. Traditional approaches utilize classifiers such as Support Vector Machines, Decision Trees, Random Forests, and Neural Networks to identify malicious activities. While deep learning-based models demonstrate high detection accuracy, their high computational and memory requirements limit their applicability in IoT scenarios.

Feature selection techniques such as Information Gain, Chi-Square tests, and Recursive Feature Elimination have been employed to reduce dimensionality and improve classifier performance. However, many studies rely on outdated datasets or do not evaluate computational overhead, which is critical for IoT systems.

Furthermore, existing IDS solutions often lack scalability and real-time performance evaluation, making them unsuitable for dynamic IoT networks. Therefore, a lightweight intrusion detection framework that integrates efficient feature selection with computationally efficient machine learning models remains an open research challenge.

Table 1. Comparison of existing intrusion detection approaches for IoT networks

Author & Year	Technique Used	Dataset	Key Findings	Limitations
Moustafa & Slay (2015)	Traditional ML classifiers	UNSW-NB15	Improved detection accuracy	High computational overhead
Sicari et al. (2015)	IoT security framework	Conceptual	Identified IoT security challenges	No real-time evaluation
Khan et al. (2020)	Hybrid ML-based IDS	NSL-KDD	High detection rate	Not optimized for IoT constraints
Zhang et al. (2021)	ML-based lightweight IDS	Custom dataset	Reduced false positives	Limited scalability
Proposed Work	Lightweight ML + Feature Selection	UNSW-NB15	High accuracy with low overhead	Future scope for real-time deployment

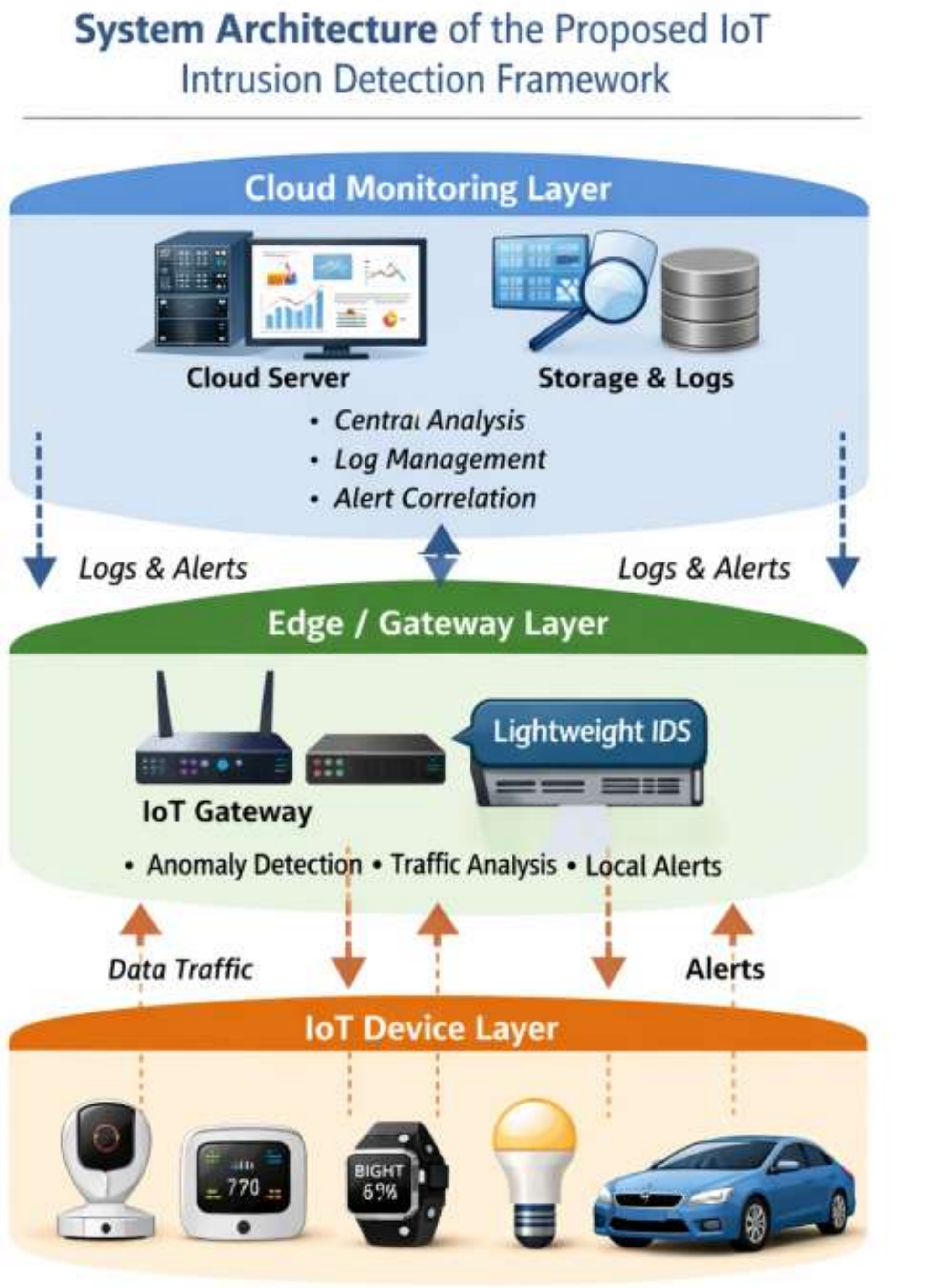

Figure 1: *System architecture of the proposed IoT intrusion detection framework.*

3 Proposed Methodology

3.1 System Architecture

The proposed intrusion detection framework consists of three layers:

- **IoT Device Layer:** Comprising sensors and smart devices that generate network traffic
- **Edge/Gateway Layer:** Hosts the lightweight IDS for traffic analysis and intrusion detection

- **Cloud/Monitoring Layer:** Responsible for logging, visualization, and administrative control

Deploying the IDS at the edge layer reduces detection latency and avoids overloading IoT devices.

3.2 Dataset Description

The UNSW-NB15 dataset is used for experimental evaluation. It includes both normal and malicious network traffic, covering attack categories such as DoS, Exploits, Fuzzers, and Reconnaissance. The dataset provides realistic traffic patterns suitable for evaluating intrusion detection systems in IoT environments.

Table 2. Characteristics of the UNSW-NB15 dataset

Attribute	Description
Total Records	~2.5 million
Features	49 network traffic features
Attack Types	DoS, Exploits, Fuzzers, Reconnaissance, Generic
Normal Traffic	Yes
Data Type	Realistic synthetic traffic
Usage	Intrusion detection evaluation

3.3 Data Preprocessing

The preprocessing phase involves:

- Removal of redundant and irrelevant attributes
- Handling missing values
- Normalization of numerical features
- Encoding of categorical attributes

These steps improve data quality and classifier performance.

3.4 Feature Selection

To reduce computational complexity, feature selection is performed using Information Gain and Chi-Square techniques. Only the most significant features contributing to intrusion detection are retained, enabling efficient model training and inference.

3.5 Machine Learning Models

The following lightweight classifiers are evaluated:

- Decision Tree

- Random Forest
- Support Vector Machine
- Naïve Bayes

These models are selected for their balance between accuracy and computational efficiency.

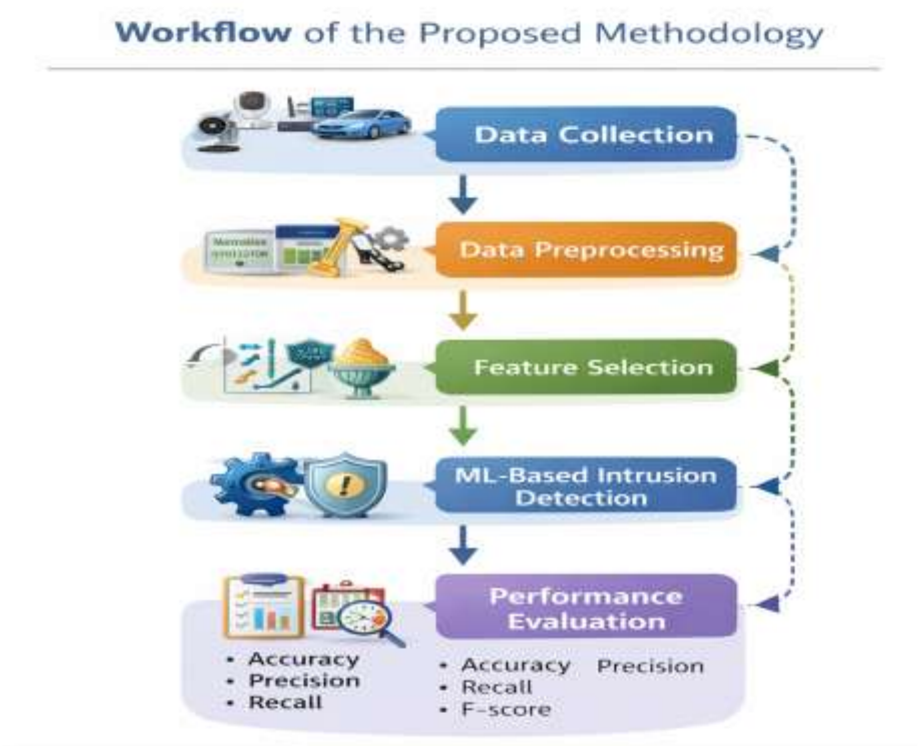

Figure 2: *Workflow of the proposed methodology, including data collection, preprocessing, feature selection, machine learning-based intrusion detection, and performance evaluation*

---

4 Experimental Setup

Experiments are conducted using Python and the Scikit-learn library. The dataset is divided into training and testing sets. Performance is evaluated using accuracy, precision, recall, F1-score, false positive rate, and detection time.

---

5 Results and Discussion

Experimental results indicate that feature selection significantly reduces computational overhead without compromising detection accuracy. Among the evaluated classifiers, Random Forest and Decision Tree models demonstrate superior performance in terms of accuracy and detection time. The proposed framework achieves improved detection efficiency compared to traditional intrusion detection approaches, making it suitable for real-time IoT security applications.

Table 3. Performance comparison of lightweight ML classifiers

Classifier	Accuracy (%)	Precision	Recall	F1-Score	Detection Time (ms)
Naïve Bayes	89.4	0.88	0.87	0.87	14
SVM	91.6	0.90	0.91	0.90	28
Decision Tree	94.2	0.94	0.93	0.93	12
Random Forest	**96.1**	**0.96**	**0.95**	**0.95**	18

6 Conclusion and Future Work

This paper proposed a lightweight machine learning–based intrusion detection system designed for resource-constrained IoT networks. By integrating feature selection with efficient machine learning classifiers, the proposed framework achieves high detection accuracy while minimizing computational overhead. Experimental results validate the effectiveness of the framework for real-time IoT security.

Future work will extend this framework using federated learning and blockchain-based security mechanisms to enhance privacy, scalability, and decentralization.

Declarations

Funding

The authors did not receive any funding for this research.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

The datasets used in this study are publicly available.

Ethical Approval

This article does not involve human participants or animals.

References

1. Moustafa, N., Slay, J.: UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Military Communications and Information Systems Conference*, pp. 1–6 (2015)
2. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks* **76**, 146–164 (2015)
3. Buczak, A.L., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials* **18**(2), 1153–1176 (2016)
4. Zhang, Y., Chen, M., Li, S.: Lightweight intrusion detection for IoT using machine learning. *Wireless Networks* **27**, 1231–1244 (2021)

5. Khan, M.A., Karim, M., Kim, Y.: A scalable and hybrid intrusion detection system based on deep learning for IoT networks. *Future Generation Computer Systems* **102**, 720–735 (2020)
6. Alrawashdeh, K., Purdy, C.: Toward an online anomaly intrusion detection system based on deep learning. *International Conference on Machine Learning and Applications*, pp. 195–200 (2016)
7. Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **5**, 21954–21961 (2017)
8. Javaid, A., Niyaz, Q., Sun, W., Alam, M.: A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, pp. 21–26 (2016)
9. Verma, A., Ranga, V.: Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications* **111**, 2287–2310 (2020)
10. Ferrag, M.A., Maglaras, L., Janicke, H., Smith, R.: Security for 5G and IoT: A survey. *Computer Communications* **146**, 136–163 (2019)
11. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* **78**, 544–546 (2018)
12. Shafiq, M., Yu, X., Laghari, A.A., Yao, L., Karn, N.K., Abdessamia, F.: Network traffic classification techniques and comparative analysis using machine learning algorithms. *Future Generation Computer Systems* **101**, 551–568 (2019)
13. Raza, S., Wallgren, L., Voigt, T.: SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks* **11**(8), 2661–2674 (2013)
14. Diro, A.A., Chilamkurti, N.: Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems* **82**, 761–768 (2018)
15. Larriva-Najarro, D., et al.: Feature selection techniques for intrusion detection systems: A survey. *Applied Sciences* **10**(4), 1–23 (2020)
16. Nguyen, T.T., Reddi, V.J.: Deep reinforcement learning for cyber security. *IEEE Communications Surveys & Tutorials* **22**(4), 2455–2476 (2020)
17. Zhou, C.V., Leckie, C., Karunasekera, S.: A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security* **29**, 124–140 (2010)
18. Sommer, R., Paxson, V.: Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, pp. 305–316 (2010)
19. Kim, G., Lee, S., Kim, S.: A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications* **41**, 1690–1700 (2014)
20. Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D.: Twenty security considerations for cloud-supported IoT. *IEEE Internet of Things Journal* **3**(3), 269–284 (2016)
21. Alasmary, W., Zhuang, W.: Mobility impact in IoT security. *IEEE Wireless Communications* **25**(6), 88–94 (2018)
22. Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. *Journal of Network and Computer Applications* **60**, 19–31 (2016)
23. Patcha, A., Park, J.M.: An overview of anomaly detection techniques. *Computer Networks* **51**, 3448–3470 (2007)
24. Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z.: A roadmap for security challenges in Internet of Things. *Digital Communications and Networks* **4**, 118–137 (2018)
25. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J.: Survey of intrusion detection systems. *Computers & Security* **77**, 51–65 (2018)