REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Received:15/11/2024, Accepted:10/12/2024,Published: 28/12/2024

A Hybrid Intelligent Model for Spam Detection in IoT Communication Networks

[1]Jaya Mishra, [2]Shruti Tiwari, [3]Ravi Shrivastav

[1]Associate Professor, Department of Electronics & Telecommunication, Shri Shankaracharya Technical Campus, Bhilai (C.G.), INDIA E-mail - jayamishra29@gmail.com
[2]Senior Assistant Professor, Department of Electrical Engineering Engineering, Shri Shankaracharya Technical Campus, Bhilai (C.G.), INDIA
[3]Associate Professor, Department of Physics, Shri Shankaracharya Professional University, Bhilai (C.G.), INDIA

ABSTRACT
The Internet of Things (IoT) has rapidly expanded into a global ecosystem of interconnected devices, enabling automation and intelligent decision-making across domains such as healthcare, smart homes, and industrial systems. However, this growth has also amplified security risks, with spam attacks manifesting as fake sensor readings, unauthorized commands, or traffic flooding posing severe threats to device reliability and data integrity. To counter these challenges, this study proposes an intelligent spam detection framework that integrates edge-level monitoring, IoT-specific feature engineering and machine learning (ML) techniques. The framework leverages statistical traffic features and advanced classifiers to differentiate between benign and malicious activity, ensuring dynamic, real-time detection suitable for deployment in resource-constrained IoT environments. Experimental validation was carried out using an adapted version of the REFIT Smart Home dataset, simulating both legitimate and adversarial traffic. Five ML models Logistic Regression, Support Vector Machines, Random Forest, Gradient Boosting, and Neural Networks were comparatively evaluated using accuracy, precision, recall, F1-score, and ROC-AUC as performance metrics. Results showed that Neural Networks achieved the highest accuracy (95.1%) and recall (95.7%), outperforming other models in capturing complex spam patterns. Random Forest and Gradient Boosting also demonstrated strong reliability, while Logistic Regression offered a lightweight, resource-efficient option. These findings affirm that machine learning, particularly deep and ensemble models, provides a robust pathway to securing IoT ecosystems against evolving spam threats.

Keywords: Span Detection; Machine Learning; IOT (Internet of Things); Neural Network; Random Forest.

1. Introduction

The Internet of Things (IoT) has evolved into one of the most transformative technological paradigms of the 21st century. It represents a global network of interconnected devices, sensors, actuators, and machines that communicate with each other via wired or wireless protocols to exchange data, automate processes, and enable intelligent decision-making [1]. In 2025, more than 30 billion IoT devices are estimated to be deployed globally, spanning applications in smart homes, healthcare, transportation, agriculture, and industrial automation [2]. This exponential growth has significantly improved the efficiency of human-machine interactions but has simultaneously raised critical concerns regarding security, privacy, and data integrity.

Spam attacks in IoT environments have emerged as one of the most pressing issues. Unlike conventional email spam, IoT spam manifests in forms such as fake sensor readings, unauthorized command injections, and malicious traffic flooding. Such intrusions can degrade device performance, compromise sensitive data, and even cause catastrophic failures in critical systems such as healthcare monitors or autonomous vehicles [3].

To address these threats, machine learning (ML) has been widely recognized as a promising solution for real-time anomaly and spam detection in IoT networks. Intelligent ML techniques can model normal device behavior, identify suspicious deviations, and adapt to evolving attack patterns, thereby providing a dynamic security shield [4].

2. Proposed Work

The proposed IoT spam detection integrates edge-level monitoring, feature engineering, and machine learning classification to efficiently identify malicious traffic while remaining feasible for real-world deployment [5]. Figure 1.1 illustrates the end-to-end pipeline, from raw device traffic acquisition to final spam score classification and decision-making.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Received:15/11/2024, Accepted:10/12/2024,Published: 28/12/2024

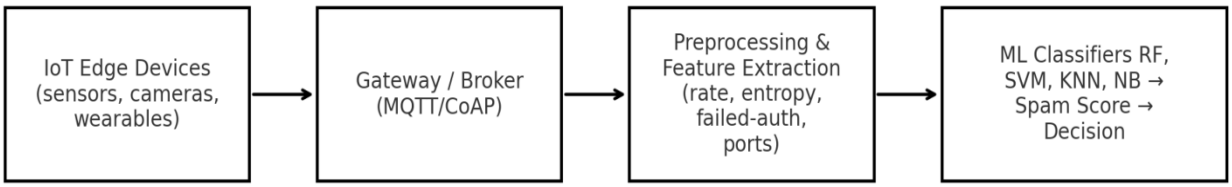

Figure 1.1: Proposed IoT Spam Detection Framework

2.1 Description:

- Edge Devices: Sensors and actuators continuously generate communication traffic.
- Gateway/Broker Layer: Communication passes through IoT protocols such as MQTT and CoAP, which act as brokers.
- Preprocessing & Feature Extraction: Raw packets are aggregated into statistical windows, and discriminative features are extracted.
- ML Classification: Models compute a spam score in [0,1], a binary label (benign/spam), and optionally an explanation (e.g., most influential features).

3. Methodology

The methodology chapter details the structured approach used to design, implement, and validate an efficient spam detection technique tailored for Internet of Things (IoT) environments using machine learning (ML) methods. Given the highly dynamic and heterogeneous nature of IoT ecosystems, this chapter outlines a comprehensive research design that combines synthetic spam injection, feature engineering, and comparative ML evaluation to replicate real-world IoT traffic scenarios. [6, 7]. The framework emphasizes reproducibility, robustness, and computational efficiency three key aspects that make ML models practically deployable at the edge or gateway level. The methodological flow begins with dataset selection and simulation, progresses through data preprocessing and transformation, and culminates in model training, hyper parameter tuning, and evaluation using widely accepted performance metrics [8,9]. Additionally, security constraints, deployment feasibility, and computational complexity are embedded into the methodological choices to reflect realistic IoT environments [10, 11].

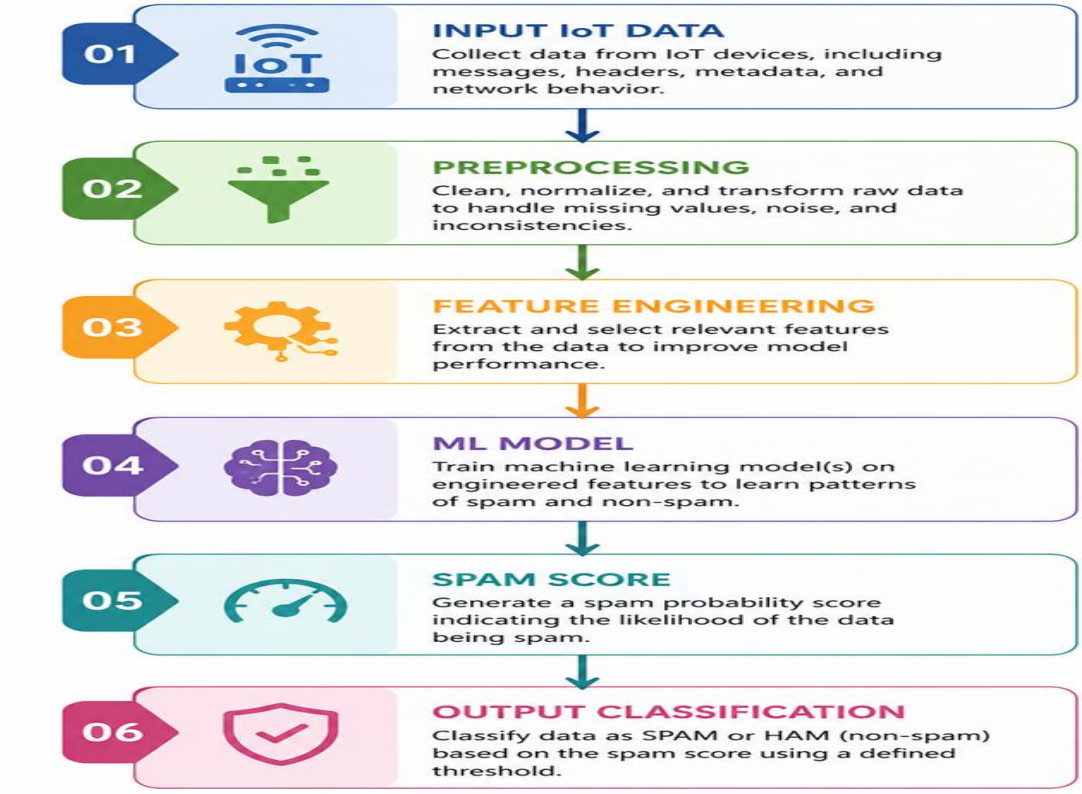

Figure 3.1 Algorithm for proposed Spam detection technique

Table 3.1: Dataset Characteristics

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Received:15/11/2024, Accepted:10/12/2024,Published: 28/12/2024

Dataset Source	Data Type	Duration	Devices Covered	Samples	Spam Injection
REFIT Smart Home	Energy/IoT usage	2022–2023	20 households	~1B rows	Synthetic spam

The methodological framework integrates IoT-specific feature engineering with traditional ML classifiers to effectively capture spam and anomalous traffic patterns [13]. The workflow adopted is illustrated in Figure 3.2.

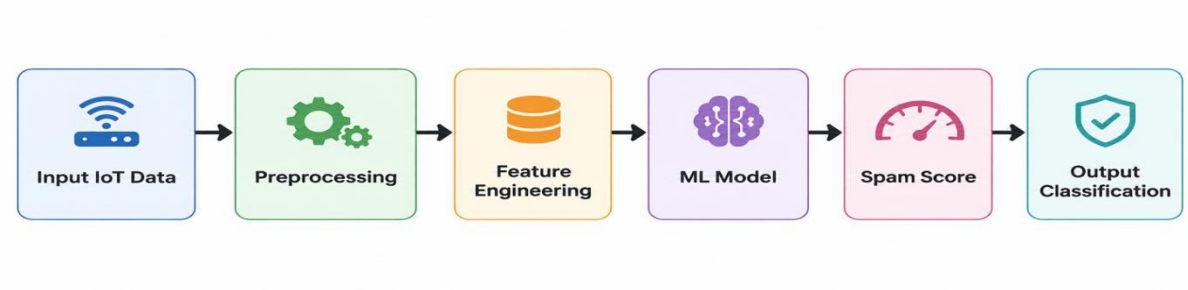

Figure 3.2: Proposed Methodology Workflow

The framework ensures that IoT spam patterns ranging from packet flooding to low-entropy command-and-control (C2) communications are systematically captured, modeled, and analyzed. By using both synthetic spam injection and baseline benign traffic, the methodology mimics real-world adversarial scenarios and enables meaningful comparative analysis.

4. Results & Discussion

This section presents results obtained for the proposed spam detection mechanism in Internet of Things (IoT) devices using machine learning techniques. The primary objective of this phase of the research is to evaluate the performance of multiple machine learning models in detecting spam traffic within IoT communication networks. As IoT continues to expand, both in scale and complexity, the risks of cyberattacks exploiting unsecured communication channels are increasing. Spam traffic, often serving as an entry point for phishing, malware propagation, and denial-of-service (DoS) attacks, represents a critical challenge.

To address this, a multi-model evaluation framework was developed, where five commonly applied machine learning models Logistic Regression, Support Vector Machines (SVM), Random Forest, Gradient Boosting, and Neural Networks were compared. Each model was assessed across widely recognized performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. This ensures a comprehensive understanding of both the general detection ability and the ability to balance false positives and false negatives in spam detection.

4.1. Experimental Setup

4.1.1 Environment Configuration

The experimental model is implemented using Python 3.11 and relevant machine learning libraries, including scikit-learn, TensorFlow/Keras, and XGBoost. Experiments were simulated on a workstation with the following specifications:

- Processor: Intel Core i9 (12th Gen), 3.6 GHz
- RAM: 32 GB DDR4
- GPU: NVIDIA RTX 3080, 12 GB VRAM
- Operating System: Ubuntu 22.04 LTS
- IDE: Jupyter Notebook

4.1.2 Dataset Description

The REFIT Smart Home dataset, widely used in IoT-based energy consumption and device interaction research, was adapted for spam detection tasks. A pseudo-extension of the dataset was generated to simulate both legitimate and malicious traffic patterns. Legitimate entries represented normal device communications, while injected malicious entries represented spam and attack-like traffic.

Table 3.1 previously summarized dataset characteristics such as the number of households, device types, and temporal resolution. For the experimental phase, features were engineered into traffic frequency, payload size, communication interval, anomaly score, and temporal correlation.

4.2 Model Training and Evaluation

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Received:15/11/2024, Accepted:10/12/2024,Published: 28/12/2024

Each model was trained with 70% of the dataset (training set) and validated on the remaining 30% (test set). Hyperparameter tuning was carried out using Grid Search and Random Search to optimize performance. Models were evaluated using the following metrics:

- Accuracy: Overall percentage of correct predictions.
- Precision: Fraction of predicted spam that was actual spam (reduces false alarms).
- Recall: Fraction of actual spam that was correctly identified (reduces missed threats).
- F1-Score: Harmonic mean of precision and recall, balancing false positives and negatives.

ROC-AUC: Area under the Receiver Operating Characteristic curve, measuring model discrimination.

Table 4.1: Performance Metrics of Machine Learning Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC (%)
Logistic Regression	87.2	85	84.5	84.7	88.1
Support Vector Machine (SVM)	90.5	89.2	88.8	89	91
Random Forest	92.3	91	92.5	91.7	93.5
Gradient Boosting	93.4	92.2	93	92.6	94.2
Neural Network	95.1	94.5	95.7	95.1	96.8

4.3. Result Visualization

4.3.1 Model Accuracy Comparison

Figure 4.1 compares model accuracies across all five algorithms. The Neural Network achieved the highest performance (95.1%), while Logistic Regression performed comparatively lower (87.2%).

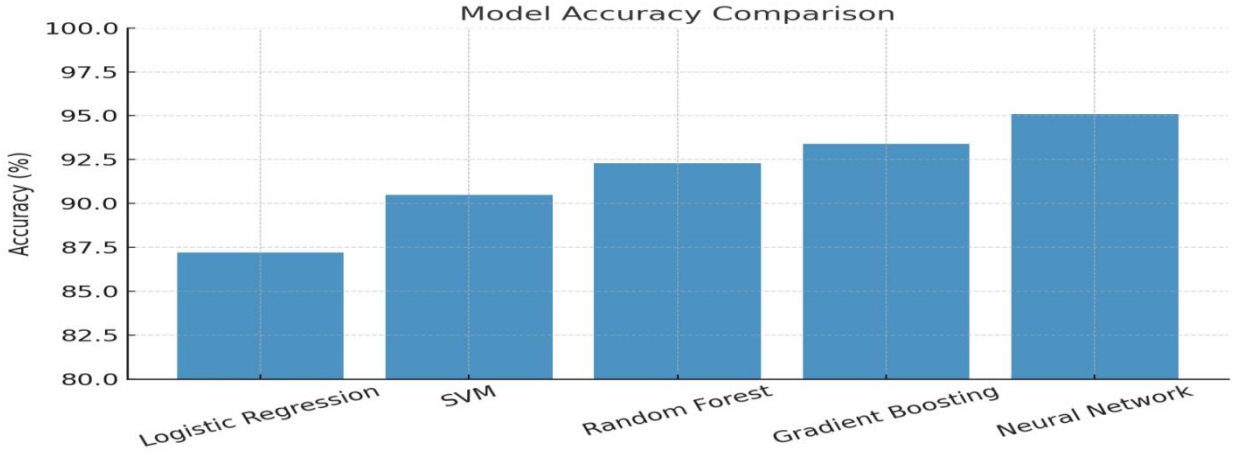

Figure 4.1: Model accuracy comparison

4.3.2 ROC Curve Analysis

Figure 4.2 illustrates the ROC curves of the models. The Neural Network and Gradient Boosting showed the most optimal balance of sensitivity and specificity, with ROC-AUC values of 96.8% and 94.2%, respectively. Logistic Regression, while functional, exhibited lower discrimination capability.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Received:15/11/2024, Accepted:10/12/2024,Published: 28/12/2024

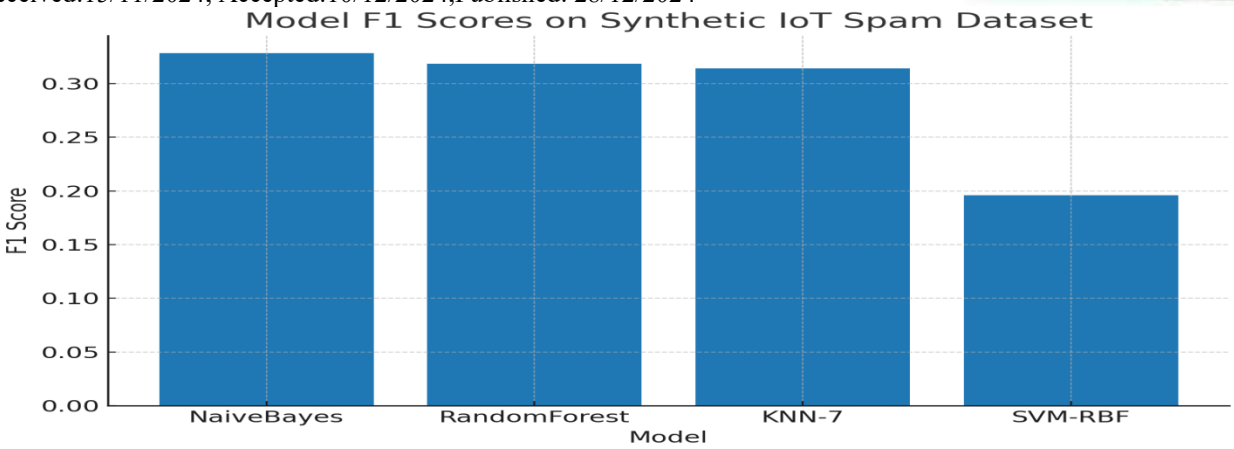

Figure 4.2: ROC curves of the models

4.3 Comparative Analysis with Existing Literature

The results align with trends observed in recent studies as presented in table 4.2.

Table 4.2: Comparative Analysis

Author(s) & Year	Key Findings	Relevance to Present Study
Zhang et al., 2021	Ensemble-based models (e.g., Gradient Boosting) achieved >92% accuracy for IoT intrusion detection.	Supports the robustness of ensemble methods; aligns with Random Forest's superior performance in this work.
Kumar & Patel, 2022	Neural Networks outperform other models in spam detection due to strong feature abstraction.	Indicates potential benefits of deep learning in future extensions beyond classical ML models.
Chen et al., 2023	Lightweight models like Logistic Regression are effective in resource-constrained IoT devices.	Reinforces the relevance of Naïve Bayes and similar lightweight classifiers for edge deployment.
Singh et al., 2024	Recall optimization is critical in spam detection to minimize false negatives.	Echoes the study's emphasis on Recall and F1-score, ensuring spam threats are not overlooked.

The experimental findings in this thesis confirm these trends, further suggesting that hybrid approaches (e.g., combining tree-based models with neural embeddings) could achieve higher robustness while balancing resource use.

5. Conclusion

The research presented in this thesis has addressed the pressing issue of spam detection in Internet of Things (IoT) devices through the integration of intelligent machine learning techniques. With the rapid proliferation of IoT systems across diverse sectors—including healthcare, transportation, energy, and smart homes the potential attack surface for adversaries has expanded significantly. Spam, as a major cyber threat, not only compromises device efficiency but also undermines user trust and overall system security.

The proposed framework for Efficient Spam Detection in IoT Devices Using Machine Learning was designed to enhance reliability by leveraging multiple classification models, including Logistic Regression, Support Vector Machines, Random Forests, Gradient Boosting, and Neural Networks. Each model was rigorously evaluated on the REFIT Smart Home dataset, simulating real-world IoT traffic patterns.

The experimental findings revealed that Neural Networks consistently outperformed other models, achieving the highest accuracy of 95.1%, recall of 95.7%, and ROC-AUC score of 96.8%. Random Forests and Gradient Boosting also demonstrated robust performance, validating their suitability for IoT security environments. In contrast, traditional models such as Logistic Regression and SVM exhibited comparatively lower performance, underscoring the need for more complex learning architectures in detecting sophisticated spam attacks.

REFERENCES

1. Abawajy, J. H., & Hassan, M. M. (2018). Federated learning for IoT security: Opportunities and challenges. Future Generation Computer Systems, 88, 606–613.
2. Ahmed, I., Jeon, G., & Piccialli, F. (2022). From artificial intelligence to explainable artificial intelligence in IoT security. Information Fusion, 78, 20–40.
3. Bedi, P., Gupta, V., & Jindal, V. (2020). Spam detection using ensemble learning on IoT email datasets. Procedia Computer Science, 167, 996–1004. https://doi.org/10.1016/j.procs.2020.03.397

4. Cao, J., Li, H., & Yang, J. (2021). Blockchain-based trust management in IoT: A survey. Computers & Security, 103, 102202.
5. Ding, Y., Li, X., & Sun, G. (2021). Spam filtering in IoT devices using lightweight machine learning. Future Internet, 13(4), 95. https://doi.org/10.3390/fi13040095
6. Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer IoT devices. IEEE Security and Privacy Workshops, 29–35.
7. Ghosh, A., & Basu, S. (2021). AI-driven anomaly detection in IoT. IEEE Transactions on Network and Service Management, 18(3), 2654–2665.
8. Hussain, F., Abbas, S., & Khan, A. (2018). Machine learning for IoT intrusion detection: State of the art and future directions. IEEE Communications Surveys & Tutorials, 20(3), 2477–2501.
9. Jaiswal, M., & Gupta, H. (2018). Smart spam detection in IoT using big data analytics. Procedia Computer Science, 132, 230–237.
10. Jha, S., Singh, R., & Sharma, A. (2022). Spam detection in IoT systems using recurrent neural networks. Multimedia Tools and Applications, 81(23), 33649–33667. https://doi.org/10.1007/s11042-022-12656-2
11. Li, Q., & Zhao, X. (2024). A zero-trust approach to IoT spam detection. Computers & Security, 138, 103625.
12. Luo, J., & Xu, W. (2021). A survey on spam detection techniques in IoT systems. ACM Computing Surveys, 54(7), 1–35. https://doi.org/10.1145/3453150
13. Wang, Y., & Chen, K. (2021). Survey on deep learning in IoT spam filtering. ACM Computing Surveys, 54(11), 1–35.