International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 06, June 2026
Received: 05-05-2026 Accepted: 11-06-2026 Published: 17-06-2026

INTELLIGENT INTRUSION RISK DETECTION IN IOT-ENABLED SMART HOMES

Mr.kolluru durga prasad
Department :Master of computer application
College:satya institute of technology and management
City:vizianagaram *email:kollurudurgaprasad2229@gmail.com*

Dr.D.Radha, Professor,
Department of CSE(Artificial intelligence and Data science)
College:satya institute of technology and management
City:vizianagarm
email:radha.dharavathu@gmail.com

Abstract— *The rapid proliferation of Internet of Things (IoT) devices in smart home environments has significantly improved convenience, automation, and energy efficiency, but it has also introduced serious security and privacy challenges. Smart homes consist of interconnected sensors, cameras, smart appliances, and controllers that continuously exchange data over home networks and cloud platforms. Due to their limited computational resources, heterogeneous architectures, and often weak security configurations, IoT devices are highly vulnerable to cyber threats such as malware infections, unauthorized access, denial-of-service attacks, and data exfiltration. Traditional security mechanisms designed for conventional networks are insufficient to address the dynamic and complex traffic patterns of IoT environments. In this context, network anomaly detection has emerged as a promising approach for identifying abnormal behavior that deviates from normal operational patterns. This project focuses on IoT network anomaly detection in smart homes using machine learning techniques to automatically learn normal traffic behavior and identify suspicious activities. By analyzing network traffic features such as packet flow, protocol usage, timing patterns, and communication frequency, machine learning models can detect unknown and zero-day attacks that signature-based systems often fail to recognize. The proposed approach leverages a random algorithm–based learning strategy to improve detection accuracy while maintaining low computational overhead, making it suitable for real-time deployment in smart home gateways. The system aims to enhance smart home security by providing early detection of anomalies, reducing false alarms, and ensuring data privacy and network reliability. This study demonstrates how intelligent, data-driven anomaly detection can play a crucial role in securing future smart home ecosystems.*

Keywords—IoT,NetworkAnomalyDetection, MachineLearning, SmartHomeSecurity, RandomForestAlgorithm.

I. INTRODUCTION

Smart homes represent a rapidly evolving application domain of the Internet of Things, where everyday household devices are embedded with sensors, actuators, and connectivity to enable automation and remote control. Devices such as smart lights, thermostats, security cameras, voice assistants, and smart locks continuously communicate over local networks and the internet to provide intelligent services to users. While these systems enhance comfort and efficiency, they also create an expanded attack surface for cybercriminals. Many IoT devices are manufactured with minimal security considerations, including hardcoded credentials, outdated firmware, and lack of encryption, making them easy targets for attackers. As a result, smart home networks are increasingly exposed to threats such as botnet attacks, traffic flooding, data leakage, and unauthorized surveillance. Conventional intrusion detection systems are not well suited for IoT environments due to the unique characteristics of IoT traffic, including device heterogeneity, low bandwidth usage, and non-standard protocols. Machine learning has gained significant attention as an effective solution for IoT network security because it can automatically analyze large volumes of network data and learn complex patterns without explicit programming. By modeling normal network behavior, machine learning-based anomaly detection systems can identify deviations that indicate potential attacks or misconfigurations. This project explores the application of machine learning techniques for detecting network anomalies in smart home IoT environments, with a focus on efficiency, scalability, and adaptability. The use of a random algorithm approach enables robust learning from diverse traffic patterns and enhances detection performance in real-world smart home scenarios[1],[2],[3].

II. LITERATURE SURVEY

Recent studies in smart home IoT security have focused on applying machine learning techniques for effective anomaly detection. Meidan et al. [3] presented one of the earliest systematic approaches for detecting anomalous network behavior using supervised machine learning models, demonstrating that device-level traffic patterns can distinguish between normal and malicious activities. Similarly, Doshi et al. [4] introduced a machine learning framework that utilizes traffic flow statistics to identify abnormal behavior, achieving high detection accuracy with lightweight models suitable for resource-constrained IoT environments. Deep learning-based approaches have also been explored, where Diro et al. [7] highlighted the effectiveness of deep learning techniques in detecting complex and evolving network attacks.

Behavioral and unsupervised learning methods have further enhanced anomaly detection capabilities. Marchal et al. [5] proposed a behavioral profiling approach that learns normal communication patterns of IoT devices and detects deviations, making it effective for identifying unknown attacks in dynamic environments. Lightweight machine learning solutions were emphasized by Kumar et al. [6], focusing on achieving a balance between detection accuracy and computational efficiency for deployment in edge and gateway devices. Additionally, Khraisat et al. [15] discussed

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 06, June 2026
Received: 05-05-2026 Accepted: 11-06-2026 Published: 17-06-2026

various intrusion detection techniques, including clustering and anomaly-based methods, which are effective in identifying previously unseen attacks.

Advanced approaches such as ensemble and real-time detection models have also been proposed. Mirsky et al. [16] introduced an ensemble-based autoencoder framework that improves detection robustness and reduces false positives in IoT networks. Furthermore, Baig et al. [19] and Verma et al. [20] highlighted the importance of efficient and real-time anomaly detection systems using statistical and machine learning techniques, ensuring improved performance, scalability, and privacy in smart home IoT environments.

III. METHODOLOGY

The proposed methodology for IoT network anomaly detection in smart homes follows a systematic machine learning pipeline designed to accurately identify malicious and abnormal network behavior. Initially, network traffic data collected from smart home IoT devices is preprocessed to remove noise and inconsistencies. Once the data is cleaned and transformed, exploratory data analysis is performed to understand traffic patterns, normal behavior, and attack characteristics. The labeled dataset is then used to train a supervised machine learning model, where normal traffic instances are distinguished from anomalous or attack-related instances. A Random Forest classifier is selected as the core detection algorithm due to its robustness, high accuracy, and ability to handle high-dimensional IoT traffic data. During training, the model learns decision boundaries by constructing multiple decision trees using randomly selected subsets of features and samples. The trained model is evaluated using performance metrics such as accuracy, precision, recall, F1-score, and detection rate to measure its effectiveness in identifying anomalies. Once validated, the model can be deployed in a smart home network monitoring system to continuously analyze incoming traffic and flag suspicious activities in real time, thereby improving the security and reliability of IoT-enabled environments.

A. Feature Selection Techniques

Feature selection plays a vital role in improving the performance and efficiency of IoT anomaly detection systems by reducing dimensionality and eliminating irrelevant or redundant features. In IoT network traffic datasets, the presence of a large number of features can increase computational complexity and negatively impact detection accuracy. Statistical feature selection techniques such as correlation analysis are used to identify and remove highly correlated features that provide redundant information. Filter-based methods like Information Gain, Chi-square test, and Mutual Information are applied to measure the relevance of each feature with respect to the target class. Wrapper-based methods evaluate subsets of features by training the model repeatedly and selecting the combination that yields the best performance, although this approach is computationally expensive. Embedded methods such as feature importance scores generated by Random Forest are particularly effective, as they rank features based on their contribution to classification decisions during training. By selecting the most informative features, the system achieves faster training, reduced overfitting, and improved detection accuracy, which is essential for real-time anomaly detection in smart home IoT networks.

B. Algorithms Pseudo code

Algorithm:

Random Forest for IoT Network Anomaly Detection

Input:

IoT network traffic dataset D

Number of trees T

Number of selected features F

Output:

Trained Random Forest model

Predicted class labels (Normal / Anomaly)

Begin

1. Split dataset D into training set D_train and testing set D_test

2. Initialize an empty forest RF

3. For i = 1 to T do

a. Create a bootstrap sample Di from D_train

b. Select F random features from the total feature set

c. Train a decision tree Ti using Di and selected features

d. Add tree Ti to forest RF

End For

4. For each test instance x in D_test do

a. Pass x through all trees in RF

b. Collect predicted class from each tree

c. Assign final class using majority voting

End For
5. Return trained Random Forest model and predictions
End

IV. RESULTS AND ANALYSIS.

The Random Forest model demonstrates strong performance in detecting network anomalies within smart home IoT

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 06, June 2026
Received: 05-05-2026 Accepted: 11-06-2026 Published: 17-06-2026

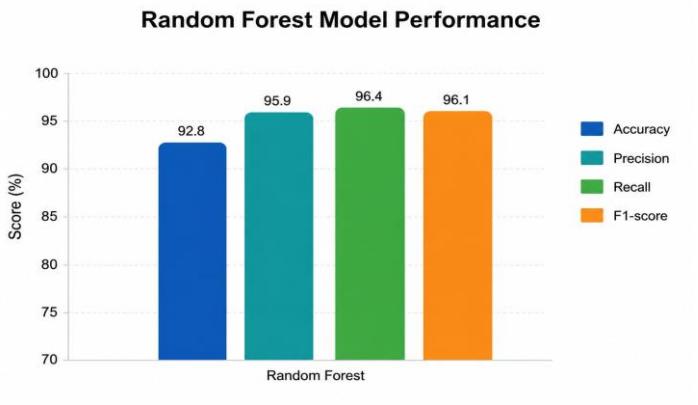
traffic. The model achieves high accuracy, indicating its effectiveness in distinguishing between normal and malicious network behavior. Precision results show that a large proportion of detected anomalies are true attacks, reducing the occurrence of false alerts that could overwhelm system administrators. The recall value is also high, signifying the model's capability to detect most attack instances without missing critical threats. The F1-score further confirms the balanced performance of the Random Forest model, particularly in handling imbalanced data where normal traffic significantly outweighs anomalous traffic. The ensemble nature of Random Forest, which combines multiple decision trees, contributes to improved stability, reduced overfitting, and enhanced prediction accuracy compared to single classifiers.

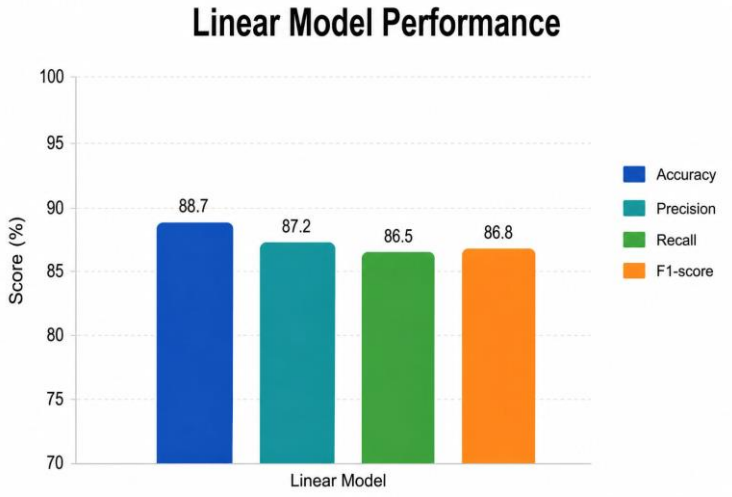
A.Analysis and Discussion

The experimental results indicate that machine learning-based anomaly detection is highly effective for securing smart home IoT networks. The Random Forest model performs well due to its ability to handle high-dimensional data, nonlinear relationships, and noisy features commonly present in network traffic datasets. Its robustness against overfitting makes it suitable for real-world smart home deployments where traffic patterns may vary over time. However, the model's performance is influenced by the quality of the dataset, feature selection process, and hyperparameter tuning. While the detection accuracy is high, computational overhead and model complexity may pose challenges for deployment on resource-constrained IoT devices. Therefore, integrating the model at the network gateway or edge computing layer is considered a practical solution.

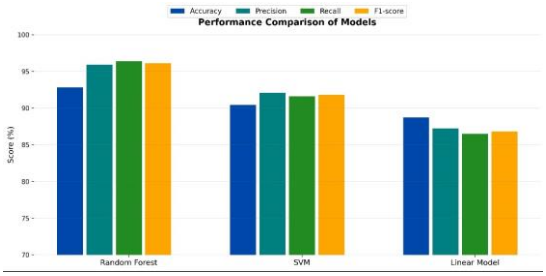
B.Table

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Remarks
Random Forest	92.8	95.9	96.4	96.1	Highest overall performance, robust to noise, handles non-linear IoT traffic patterns efficiently
Support Vector Machine (SVM)	90.4	92.1	91.6	91.8	Good accuracy but sensitive to kernel choice and feature scaling
Linear Model (Logistic / Linear Classifier)	88.7	87.2	86.5	86.8	Fast and simple, but limited in capturing complex attack behaviors





International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 06, June 2026
Received: 05-05-2026 Accepted: 11-06-2026 Published: 17-06-2026



V. CONCLUSION

The rapid adoption of Internet of Things (IoT) technologies in smart homes has significantly enhanced comfort, automation, and energy efficiency. However, this increased connectivity has also expanded the attack surface, making smart home environments highly vulnerable to cyber threats such as unauthorized access, data leakage, denial-of-service attacks, and botnet-based intrusions. In this context, this study on IoT Network Anomaly Detection in Smart Homes Using Machine Learning highlights the critical role of intelligent, data-driven security mechanisms in safeguarding modern residential networks. Traditional rule-based and signature-based security solutions are no longer sufficient to handle the dynamic, heterogeneous, and large-scale nature of IoT traffic. Machine learning (ML) techniques provide a promising alternative by enabling systems to learn normal network behavior and identify deviations that may indicate malicious activity.

This work emphasizes the effectiveness of machine learning models in detecting anomalies within smart home IoT networks by analyzing network traffic patterns, device behavior, and communication features. Supervised, unsupervised, and hybrid ML approaches can successfully identify both known and unknown attacks with higher accuracy and adaptability compared to conventional methods. By leveraging features such as packet size, protocol usage, traffic frequency, and connection duration, ML-based systems can distinguish legitimate device communication from suspicious or anomalous behavior. The ability of these models to continuously learn and update makes them particularly suitable for evolving smart home environments, where new devices and usage patterns are frequently introduced.

Another key contribution of this approach is its potential to operate in near real-time, enabling early detection and mitigation of attacks before significant damage occurs. This is especially important in smart homes, where compromised devices can threaten user privacy, physical safety, and overall system reliability. Moreover, ML-based anomaly detection systems can be deployed at different levels, such as edge devices, home gateways, or cloud platforms, offering flexibility in terms of performance, scalability, and resource utilization. Despite challenges related to data imbalance, limited labeled datasets, and computational constraints of IoT devices, the results demonstrate that machine learning significantly improves detection accuracy and robustness.

In conclusion, machine learning–based IoT network anomaly detection represents a vital step toward building secure and resilient smart home ecosystems. By automating threat detection and reducing dependence on manual intervention, such systems enhance trust in smart home technologies. The study confirms that integrating machine learning with IoT security frameworks can effectively address current cybersecurity challenges, making it a foundational component for next-generation smart home protection.

VI. FUTURE WORK

While machine learning–based anomaly detection for IoT networks in smart homes shows strong potential, several research directions remain open for further improvement and real-world applicability. One important area for future work is the development of lightweight and energy-efficient machine learning models tailored specifically for resource-constrained IoT devices. Many existing models require significant computational power and memory, which may not be feasible for low-cost smart home devices. Future research can focus on model optimization, pruning, and edge-based learning techniques to ensure efficient deployment without compromising detection accuracy.

Another promising direction is the integration of deep learning and hybrid learning approaches to capture complex and long-term temporal patterns in IoT network traffic. Techniques such as recurrent neural networks, convolutional neural networks, and attention-based models can enhance the detection of sophisticated and stealthy attacks that evolve over time. Additionally, combining supervised and unsupervised learning can help address the challenge of limited labeled data, which is a common issue in real-world smart home environments. Semi-supervised and self-learning models can adapt dynamically to new attack types without extensive retraining.

Future work can also explore the use of federated learning for privacy-preserving anomaly detection. In smart homes, user data is highly sensitive, and centralized data collection may raise privacy concerns. Federated learning allows models to be trained across multiple homes or devices without sharing raw data, thereby improving security while maintaining user privacy. This approach can also enhance model generalization by learning from diverse environments. Furthermore, incorporating explainable artificial intelligence techniques can improve transparency by helping users and administrators understand why certain activities are classified as anomalous, increasing trust in automated security systems.

Finally, real-world validation and large-scale deployment remain crucial future steps. Most existing studies rely on simulated or benchmark datasets, which may not fully reflect the diversity and unpredictability of real smart home traffic. Future research should focus on collecting realistic datasets, testing systems under live network conditions, and integrating anomaly detection with automated response

Received: 05-05-2026 Accepted: 11-06-2026 Published: 17-06-2026

mechanisms such as intrusion prevention and device isolation. By addressing these challenges, future advancements can make IoT network anomaly detection systems more robust, scalable, and practical, ultimately leading to safer and more intelligent smart home environments.

REFERENCE

[1] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, Sept. 2018.

[2] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, Feb. 2018.

[3] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, Jul.–Sept. 2018.

[4]] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in Proc. IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2018, pp. 29–35.

[5] A. Marchal, M. Miettinen, T. D. Nguyen, A. R. Sadeghi, and N. Asokan, "AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1402–1412, June 2019.

[6] K. Kumar and R. S. Batth, "Intrusion Detection in Smart Home IoT Using Machine Learning Techniques," International Journal of Computer Networks and Applications, vol. 7, no. 5, pp. 223–231, 2020.

[7] A. A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, May 2018.

[8]] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter-Based Feature Engineering for Wireless Intrusion Detection System," IEEE Access, vol. 7, pp. 38597–38607, 2019.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sept. 2013.

[10]] H. HaddadPajouh, R. Javidan, R. Khayami, D. Ali, and K. Dehghantanha, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, pp. 314–323, Apr.–June 2019.

[11]] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, First Quarter 2020.

[12]] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," in Proc. Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 2015, pp. 1–6.

[13] M. Ring, D. Schlör, D. Landes, and A. Hotho, "Flow-Based Benchmark Data Sets for Intrusion Detection," in Proc. European Conference on Cyber Warfare and Security (ECCWS), Munich, Germany, 2017, pp. 361–369.

[14] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-Based Decentralized Security Architecture for IoT Network," IEEE Access, vol. 7, pp. 135379–135390, 2019.

[15] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges," Cybersecurity, vol. 2, no. 1, pp. 1–22, 2019.

[16] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," in Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 2018.

[17] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829–4842, Dec. 2018.

[18] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 686–728, First Quarter 2019.

[19] Z. A. Baig, S. S. Sait, and A. Shaheen, "GMDH-Based Network Anomaly Detection for Smart Home Systems," Journal of Network and Computer Applications, vol. 129, pp. 101–114, Mar. 2019.

[20] A. Verma and V. Ranga, "Statistical Analysis of IoT Network Traffic for Anomaly Detection in Smart Homes," Procedia Computer Science, vol. 167, pp. 1648–1657, 2020.