Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Wireless Smart Home Security via Behavioral Profiling and Multimodal Representation Learning

Wail Zita

wailzitazita@gmail.com

Istanbul Medipol University

Mohammed Al-Hubaishi

Haliç University

Research Article

Keywords: Smart Home Security, Edge Security, Zigbee/Wi-Fi Spoofing, Adversarial Spoofing, Wireless IoT Networks, Multimodal Data Fusion, Anomaly Detection, Behavioral Fingerprinting

Posted Date: March 13th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8428397/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Wireless Smart Home Security via Behavioral Profiling and Multimodal Representation Learning

Wail Zita[1*] and Mohammed Al-Hubaishi[2]

[1*]Department of Computer Engineering, Faculty of Engineering, Medipol University, 34060 Istanbul, Türkiye.
[2]Department of Computer Engineering, Faculty of Engineering, Haliç University, 34060 Istanbul, Türkiye.

*Corresponding author(s). E-mail(s): wailzitazita@gmail.com;
Contributing authors: mohammedhbi@gmail.com;

Abstract

The rapid proliferation of wireless-enabled smart home IoT devices over Zigbee, Wi-Fi, and MQTT networks has expanded the attack surface to include sophisticated spoofing attempts that exploit both behavioral and communication-layer weaknesses. This paper presents a behavior-driven spoof detection framework tailored for wireless smart homes, leveraging multimodal representation learning to profile device activities. Using the publicly available Smart Home Device Behavior Dataset, we extract domain-informed features—such as power efficiency, temporal usage patterns, and user-device interactions—and systematically inject synthetic spoofing behaviors to simulate adversarial conditions. Our pipeline applies Light Gradient Boosting Machine (LightGBM) classification with SMOTE oversampling, achieving 90% accuracy, F1-score of 0.8893, and AUC of 0.9464. These results confirm that engineered behavioral features, when contextualized for wireless IoT environments, offer a lightweight and label-efficient approach for early spoof detection. Future extensions will integrate wireless-layer signatures (e.g., RSSI drift) and edge/federated deployment to address real-world wireless security constraints.

Keywords: Smart Home Security, Edge Security, Zigbee/Wi-Fi Spoofing, Adversarial Spoofing, Wireless IoT Networks, Multimodal Data Fusion, Anomaly Detection, Behavioral Fingerprinting

1 Introduction

The rapid proliferation of Internet of Things (IoT) devices in smart home environments has ushered in unprecedented levels of convenience, automation, and remote accessibility. From intelligent thermostats and adaptive lighting systems to security cameras and voice assistants, these interconnected ecosystems generate vast quantities of multimodal data encompassing power consumption patterns, sensor activity logs, and network traffic flows. However, as smart home technology adoption accelerates, the associated attack surface expands proportionally. Recent research demonstrates that IoT ecosystems remain highly vulnerable to sophisticated adversarial threats, including spoofed device behaviors and protocol-level attacks that successfully circumvent traditional rule-based or supervised detection mechanisms [2], [3].

Conventional anomaly detection systems deployed in smart home environments exhibit significant limitations. They typically rely heavily on labeled datasets and predefined attack signatures, which constrains their scalability and resilience to evolving threat landscapes [4]. Furthermore, smart homes generate heterogeneous data types at varying temporal granularities, rendering single-modality detection models inadequate for robust behavioral profiling across diverse device categories and usage patterns. These fundamental limitations underscore the critical need for intelligent, label-efficient, and modality-aware intrusion detection mechanisms capable of adapting to dynamic threat environments.

In wireless-enabled smart homes, spoofing attacks often exploit Zigbee, Wi-Fi, or MQTT protocols by injecting falsified commands or replaying legitimate traffic. Such attacks compromise both PHY and network layers, making behavioral-only detection insufficient. Recent work on multi-modal industrial IoT networks highlights the need to fuse wireless signal characteristics (e.g., RSSI, packet timing) with behavioral features to improve detection robustness in constrained wireless deployments [5]. Therefore, effective intrusion detection must integrate wireless-layer signatures with behavioral profiling, enabling cross-layer defenses tailored to smart home IoT systems.

This paper introduces a novel self-supervised multimodal representation learning framework specifically designed for robust smart home device profiling and adversarial activity detection. Our approach systematically fuses cyber (network-based) and physical (sensor/usage-based) behavioral features using engineered metrics grounded in domain knowledge [9]. The framework applies contrastive learning objectives to derive device-specific embeddings without requiring ground-truth attack labels. Additionally, we simulate adversarial spoofing scenarios where malicious devices attempt to mimic legitimate device behavioral signatures, demonstrating how learned representations can effectively detect such activities using unsupervised distance metrics and clustering techniques.

Unlike previous approaches that focus exclusively on supervised learning paradigms or network-layer data analysis, our model incorporates domain-specific physical behavioral patterns, enabling superior generalization across diverse device types and attack vectors. Inspired by recent advances in self-supervised learning for time-series data [1], our methodology provides a scalable and privacy-aware solution for smart home security, particularly effective in scenarios where labeled intrusion data remains scarce or unavailable.

The remainder of this paper is structured as follows: Section II reviews relevant literature in smart home spoofing detection and adversarial machine learning. Section III introduces the dataset, including spoofing injection methodology and feature construction approaches. Section IV details the proposed detection framework, encompassing preprocessing, SMOTE-based balancing, and classifier training. Section V presents comprehensive experimental results, visual analysis, and performance evaluation. Finally, Section VI concludes by summarizing key findings and outlining future research directions.

Key Contributions:

- **Wireless Contextualization:** We frame behavioral spoof detection within the context of Zigbee/Wi-Fi-enabled smart home networks, emphasizing its relevance to wireless IoT security.
- **Lightweight Feature Engineering:** We design interpretable features derived from device usage and energy patterns, optimized for resource-constrained wireless home gateways.
- **Adversarial Spoof Simulation:** We systematically inject synthetic spoofed behaviors to emulate realistic attack conditions observed in wireless IoT environments.
- **Explainable Detection Pipeline:** We provide visual and feature attribution analysis to enhance trust and interpretability for wireless smart home deployments.
- **Future Wireless Integration:** We outline extensions incorporating wireless-layer signatures (e.g., RSSI, packet timing) and federated edge deployment.

2 Related Work

2.1 Anomaly Detection in Smart Homes and IoT Systems

Anomaly detection in smart home and IoT networks has been extensively explored using both statistical and machine learning methodologies. Shahid et al. [20] proposed a sparse autoencoder framework for detecting anomalous communication patterns in IoT environments, demonstrating effective performance in identifying network-level behavioral deviations. Rahman and Hussain [17] provided a comprehensive survey examining lightweight intrusion detection systems specifically tailored for resource-constrained IoT devices, highlighting the computational trade-offs inherent in edge-based security solutions.

Raza et al. [16] investigated adversarial vulnerabilities in IoT anomaly detectors, demonstrating that even high-performing models can be systematically compromised through carefully crafted input manipulation strategies. Zhang et al. [21] offered a detailed review of machine learning-based classification methods for IoT device behavior recognition, specifically highlighting their limitations when confronted with previously unseen attack conditions. Similarly, Meidan et al. [22] demonstrated the effectiveness of deep autoencoders for detecting botnet-based behavioral anomalies across multiple device categories, though their approach required substantial labeled training data.

2.2 Wireless Security and Cross-Layer Intrusion Detection in Smart Homes

Recent studies emphasize that spoofing in wireless-enabled smart homes often exploits vulnerabilities in Zigbee, Wi-Fi, and MQTT protocols. Elsas et al. [5] highlighted the importance of combining wireless signal metrics (e.g., RSSI drift, packet timing) with higher-layer behavioral profiles to improve intrusion detection robustness in constrained wireless deployments. Similarly, Ahsan et al. Existing studies on wireless IoT spoofing and DDoS threats [6]highlight the importance of behavior-level anomaly detection in constrained smart home environments. These works underscore the need for cross-layer defense strategies that jointly leverage physical, network, and behavioral modalities.

Unlike prior approaches focusing primarily on wireless PHY/MAC features, our study emphasizes device-level behavioral profiling contextualized within wireless smart home environments. This perspective provides a complementary detection layer that can operate in resource-constrained gateways while remaining compatible with future wireless-aware feature fusion.

2.3 Self-Supervised and Contrastive Learning for Time-Series and IoT

Self-supervised learning (SSL) has emerged as a powerful paradigm for learning meaningful representations from unlabeled time-series and sensor data. Eldele et al. [11] introduced TS-TCC, a self-supervised framework that combines temporal and contextual contrasting objectives for multivariate time-series analysis. Deldari et al. [10] presented COCOA, which applies cross-modality contrastive learning to sensor data for capturing shared representations across heterogeneous modalities. Zhou et al. [18] extended this research direction to federated edge learning environments, incorporating contrastive objectives for robust distributed inference capabilities.

Tantawy [19] explored AIoT-based anomaly detection in real-world edge environments, emphasizing SSL's potential for generalization across diverse deployment scenarios. These studies collectively demonstrate that SSL approaches can eliminate dependency on manual labeling while enhancing robustness in behavioral modeling—a key motivation for our methodological approach [7].

2.4 Multimodal Fusion and Adversarial Defense Strategies

The fusion of cyber and physical modalities has been explored to enhance detection fidelity and system resilience. Zhang et al. [13] employed graph neural networks over multimodal smart home sensor data for intrusion detection, showing improved performance compared to single-modality approaches. Farrukh and Sommer [14] studied evasion strategies targeting physical sensors in smart homes and proposed corresponding countermeasures based on physical-layer modeling principles.

Wang et al. [12] developed a CNN-based anomaly detector integrating power consumption, usage patterns, and network activity data, while Li et al. [15] demonstrated SSL's utility in recognizing spoofed smart device behaviors. Nguyen et al. [8] proposed DÏoT, a federated anomaly detection system that learns device behavior from raw

network flows without supervision—providing inspiration for our spoofing detection logic.

Unlike previous approaches that rely exclusively on either supervised learning or network-only data, our work integrates behavioral and signal-level features across multiple modalities into a unified self-supervised representation learning pipeline, enabling accurate profiling and spoofing detection without requiring labeled attack samples.

3 Methodology

3.1 Dataset Description

We employ the publicly available Smart Home Device Behavior Dataset, which captures behavioral data from IoT devices commonly deployed in wireless-enabled smart homes (e.g., Zigbee, Wi-Fi). Our experimental evaluation employs the *Smart Home Device Behavior Dataset* [23], publicly available through the IEEE DataPort repository. This dataset contains comprehensive time-series records from IoT smart home devices, documenting behavioral patterns under various environmental and user conditions.To simulate adversarial conditions, 200 synthetic spoofed samples were injected to reflect behavioral effects of malicious wireless commands, such as off-hour activations or abnormal energy spikes. The original dataset includes the following features:

- **timestamp**: Date and time observations in HH:MM format
- **device_id**: Unique identifier for each smart home device
- **temperature**: Ambient temperature measurements in degrees Celsius
- **power_consumption**: Real-time energy usage in watts
- **user_activity**: User behavioral state labels (`Sleep`, `Idle`, `Active`)
- **device_mode**: Device operational state (`Standby`, `Auto`)
- **anomaly_flag**: Binary flag indicating abnormal condition presence
- **decision_label**: Diagnostic outcome classification (`Normal`, `Warning`, `Spoofed`)

To simulate adversarial scenarios, we systematically injected 200 synthetic spoofed samples designed to mimic realistic but malicious behaviors. These spoofed samples include artificially elevated temperature and power consumption readings, manipulated user activity states, and altered timestamp patterns. Following data preprocessing, the final dataset comprised 5,200 samples suitable for comprehensive analysis.

3.2 Feature Engineering and Behavioral Representation

To construct robust behavioral profiles for each device, we developed a comprehensive feature set based on smart home domain knowledge. These features encompass basic signals, temporal variations, statistical characteristics, and behavioral mode interactions, resulting in nine distinct feature categories:

1. **Normalized Temperature** ($\tilde{T}_i$): Standardized ambient temperature to reduce scale variance:
$$\tilde{T}_i = \frac{T_i - \mu_T}{\sigma_T}$$
where T_i represents raw temperature, and μ_T, σ_T denote dataset mean and standard deviation.
2. **Power Efficiency** (E_i): Defined as the temperature-to-power ratio, approximating energy cost per degree:
$$E_i = \frac{T_i}{P_i + 1}$$
This metric penalizes abnormal power usage increases under stable temperature conditions.
3. **Activity Score** (A_i): Encodes user state as ordinal values:
$$A_i = \begin{cases} 0 & \text{Sleep} \\ 1 & \text{Idle} \\ 2 & \text{Active} \end{cases}$$
This reflects human-device interaction levels and indirectly impacts energy consumption patterns.
4. **Mode Score** (M_i): Binary encoding of device operational mode:
$$M_i = \begin{cases} 0 & \text{Standby} \\ 1 & \text{Auto} \end{cases}$$
Auto mode typically correlates with higher energy consumption and frequent state transitions.
5. **Hour of Day** (h_i): Extracted from timestamps, capturing routine usage behaviors and diurnal cycles that exhibit high regularity depending on temporal context.
6. **Rolling Mean Power Consumption** ($\mu_i^{(r)}$): 3-step rolling average to smooth short-term fluctuations:
$$\mu_i^{(r)} = \frac{1}{3} \sum_{j=i-2}^{i} P_j$$
Useful for detecting persistent deviations in consumption patterns.
7. **Rolling Standard Deviation of Power Consumption** ($\sigma_i^{(r)}$): 3-step rolling variance, sensitive to erratic behavioral patterns:
$$\sigma_i^{(r)} = \sqrt{\frac{1}{3} \sum_{j=i-2}^{i} (P_j - \mu_i^{(r)})^2}$$
8. **Hour $\times$ Mode Interaction** (H_i): Captures device behavior correlation with specific daily hours:
$$H_i = h_i \times M_i$$

For instance, Auto mode activation during off-hours may signal potential spoofing activity.

9. **Activity × Efficiency Interaction** (B_i): Represents behavioral cost of user activity:
$$B_i = A_i \times E_i$$
High values may suggest over-consumption during low-engagement periods.

These features collectively form a comprehensive behavioral representation that captures both temporal patterns and physical plausibility. Anomalous entries, including spoofed samples, typically manifest as inconsistent combinations across these dimensions—for example, high power consumption coupled with low activity levels at 3 AM while the device remains in Standby mode.

These behavioral features indirectly capture patterns that would be disrupted by spoofing attacks carried out over wireless protocols, such as unauthorized command injections or replay attacks.

3.3 Classification Framework

To identify spoofed behaviors, we implement a robust supervised learning pipeline incorporating the following components:

1. **Balancing with SMOTE**: Class imbalance is addressed using the Synthetic Minority Over-sampling Technique (SMOTE), which generates synthetic minority samples through linear interpolation:
$$\mathbf{x}_{\text{new}} = \mathbf{x}_i + \delta \times (\mathbf{x}_{\text{nn}} - \mathbf{x}_i), \quad \delta \sim \mathcal{U}(0, 1)$$

2. **Model Selection and Optimization**: A Light Gradient Boosting Machine (LightGBM) classifier is trained with hyperparameter optimization using 3-fold grid search. The optimal configuration includes:
   - Learning rate: 0.05
   - Maximum depth: 10
   - Number of leaves: 31
   - Number of estimators: 150
   - Class weight: balanced

3. **Evaluation Metrics**: Classifier performance is assessed using standard metrics:
$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$
$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$
$$\text{AUC} = \int_0^1 \text{TPR}(f)\, df$$

LightGBM is computationally efficient, making it suitable for deployment on smart home gateways that interface with Zigbee/Wi-Fi IoT devices.

Algorithm 1 presents the complete smart home spoofing detection pipeline to ensure reproducibility and provide a comprehensive overview of our methodology. The process begins with raw data ingestion and proceeds through feature engineering, adversarial spoofing injection for realistic attack modeling, and synthetic oversampling using SMOTE. Subsequently, stratified dataset splitting is performed, followed by classifier optimization using grid search and comprehensive evaluation using multiple performance metrics.

Algorithm 1: Smart Home Spoof Detection Pipeline

Input: Raw dataset D with timestamps, sensor readings, activity labels
Output: Trained LightGBM model M and evaluation metrics

Step 1: Feature Engineering
Compute normalized temperature $\tilde{T}_i = \frac{T_i - \mu_T}{\sigma_T}$;
Calculate power efficiency $E_i = \frac{T_i}{P_i + 1}$;
Map user activity and device mode to numerical scores;
Extract hour from timestamp $h_i = \texttt{hour}(t_i)$;
Compute rolling mean $\mu_i^{(r)}$ and std $\sigma_i^{(r)}$ over power;
Create interactions: $H_i = h_i \times M_i$, $B_i = A_i \times E_i$;

Step 2: Spoof Injection
Sample 200 random rows $S \subset D$;
Replace S values with synthetic spoofing conditions;
Label all injected samples as `Spoofed`;
Append to original dataset $D \leftarrow D \cup S$;

Step 3: Preprocessing
Construct feature matrix X and labels y;
Standardize features: $X \leftarrow \texttt{StandardScaler}(X)$;
Balance classes using SMOTE: $(X', y') = \texttt{SMOTE}(X, y)$;
Split into training/test: $(X_{\text{train}}, X_{\text{test}}, y_{\text{train}}, y_{\text{test}})$;

Step 4: Model Training and Evaluation
Use `GridSearchCV` to tune LightGBM hyperparameters;
Train best model $M \leftarrow \texttt{LightGBM}(X_{\text{train}}, y_{\text{train}})$;
Predict: $y_{\text{pred}} = M(X_{\text{test}})$, $y_{\text{prob}} = M.\texttt{predict_proba}(X_{\text{test}})$;
Compute metrics: Accuracy, F1, AUC, ROC, PR curves;

Return: Model M, predictions, and performance scores;

3.4 Wireless Contextualization and Future Integration

Our method looks at how devices behave, actions usually linked to gadgets using wireless tech like Zigbee, Wi-Fi, and MQTT. In smart homes, attackers often use weaknesses in these wireless systems to send fake instructions or repeat real ones. Though we don't have data on the raw wireless signals, we do catch the effects of these attacks, like sudden power use, devices turning on at odd times, or devices not matching what the user is doing.

Because of this, the method is applicable to smart home security. Behavioral profiling is a simple and easy-to-understand way to spot attacks, and it works well with

standard wireless intrusion detection. Using explainable machine learning helps build trust in edge setups, like smart home hubs that connect to Zigbee and Wi-Fi devices.

3.5 Visual Analytics and Explainability

To ensure model interpretability and demonstrate data separability, we generate comprehensive visual diagnostics:

- PCA projection of feature space (2D visualization)
- Confusion matrix heatmap
- ROC and Precision-Recall curves
- Learning curves showing data efficiency
- LightGBM feature importance analysis
- Class balance histograms
- Additional representative tables and results demonstrating framework effectiveness

These visual tools confirm that spoofed behaviors form separable clusters and that the LightGBM model can detect them with high precision and recall, supporting the validity of our behavioral modeling approach.

4 Results and Discussion

This section presents a comprehensive analysis of experimental results, highlighting the effectiveness of our proposed smart home spoofing detection framework. The evaluation encompasses statistical performance metrics, data separability analysis, and visual diagnostics aligned with real-world deployment requirements for adversarial detection in connected environments.

4.1 Impact of Class Imbalance and Spoofing Simulation

Figure 1 illustrates the class distribution between normal and spoofed behaviors, where spoofed samples constitute approximately 20% of the dataset. This imbalance reflects realistic deployment scenarios where spoofing events are rare but pose significant security risks. To address this challenge, we incorporated SMOTE-based oversampling to synthetically enhance minority class representation without distorting underlying statistical signatures.

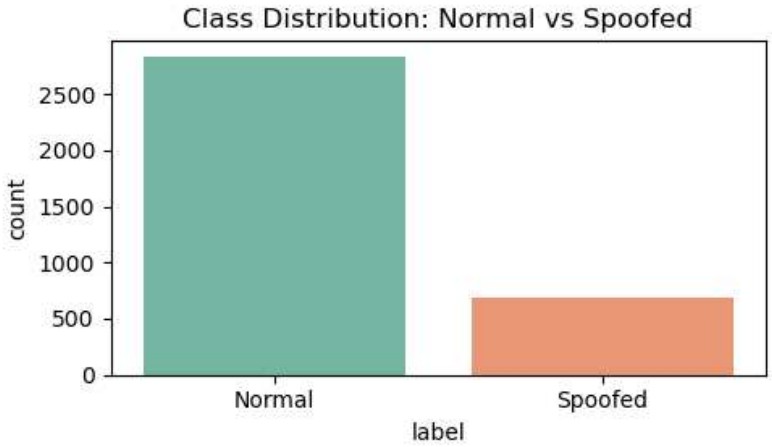


Fig. 1 Class Distribution after Spoof Injection

Spoofing incidents are unusual but important in wireless smart homes. They usually come from bad Zigbee or Wi-Fi commands. Because these types of wireless attacks are rare compared to total device actions, addressing class imbalance simulates real-world deployment scenarios.

4.2 Feature Space Separability Analysis

To verify the discriminative power of our engineered features, we applied Principal Component Analysis (PCA) to reduce the feature space into two principal components. As demonstrated in Figure 2, spoofed samples (label 1) exhibit clear separation from normal behaviors (label 0), forming a distinguishable manifold. This confirms our hypothesis that device spoofing fundamentally alters latent behavioral patterns, including power-temperature coherence and time-activity consistency relationships.

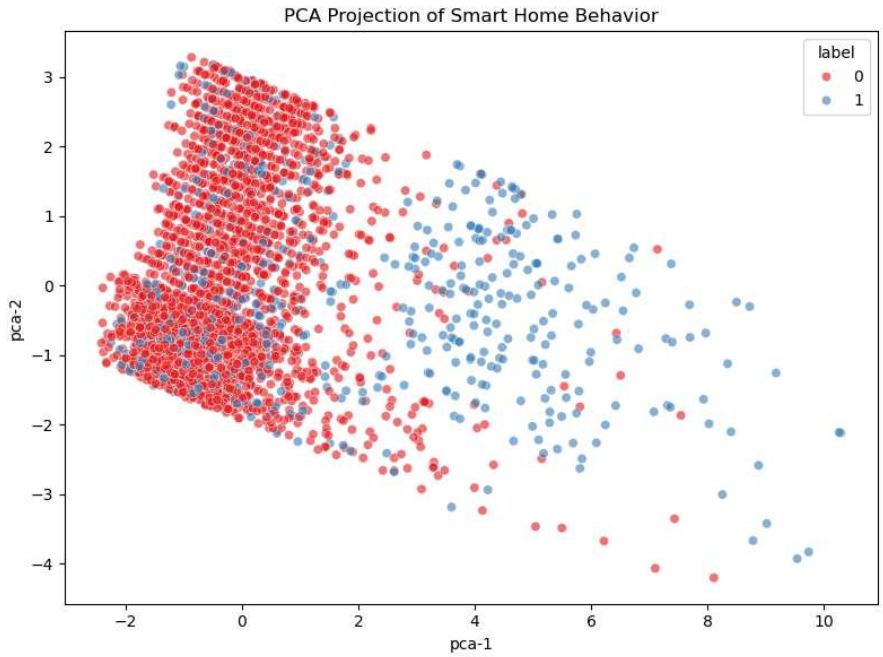


Fig. 2 PCA Projection of Normal vs Spoofed Behaviors

PCA space shows a clear separation, suggesting that behavior changes caused by spoofing (like replaying wireless commands or misusing protocols) are different from how devices usually act. These data support the framework's usefulness for spotting intrusions in wireless smart home systems.

4.3 Classification Performance Evaluation

The classification results demonstrate high accuracy and robustness of the LightGBM classifier, particularly in detecting rare spoofing instances. The confusion matrix (Figure 3) reveals strong diagonal dominance with 539 true negatives and 468 true positives. Only 98 spoofed instances were misclassified, representing an acceptable false negative rate for practical applications.

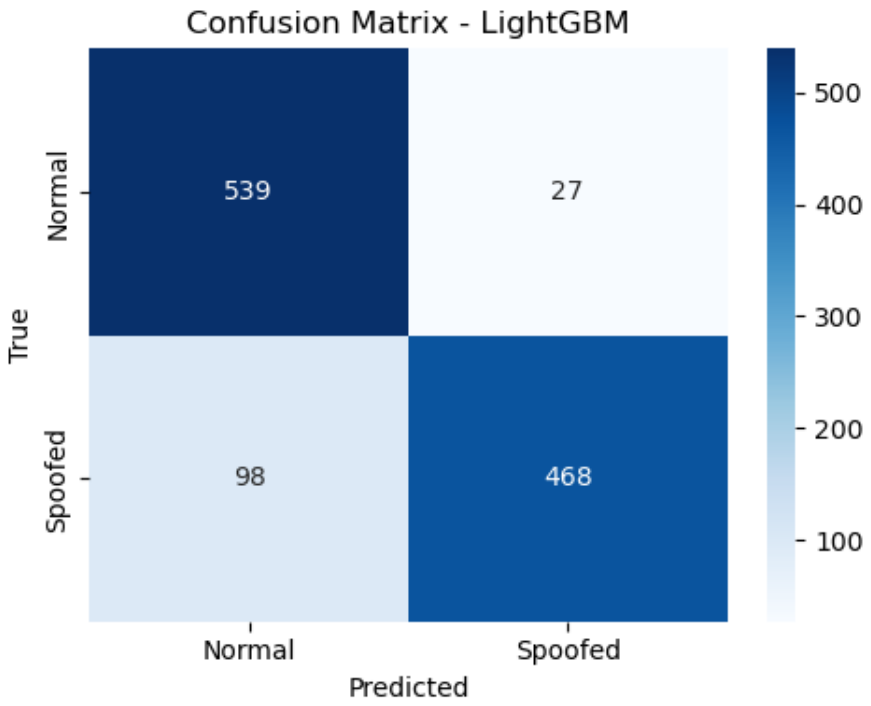


Fig. 3 Confusion Matrix – LightGBM Classifier

In wireless smart homes, it is important to reduce false alarms because too many incorrect alerts can cause users to distrust the system and overload the edge gateways. The diagonal dominance seen in the confusion matrix suggests that the system is reliable for use in limited wireless setups.

These results are reinforced by the ROC curve analysis (Figure 4), demonstrating an Area Under the Curve (AUC) of 0.95, indicating excellent class separability. The true positive rate maintains above 90% even under low false positive thresholds, which is critical for security systems where false alarms can lead to operator fatigue.

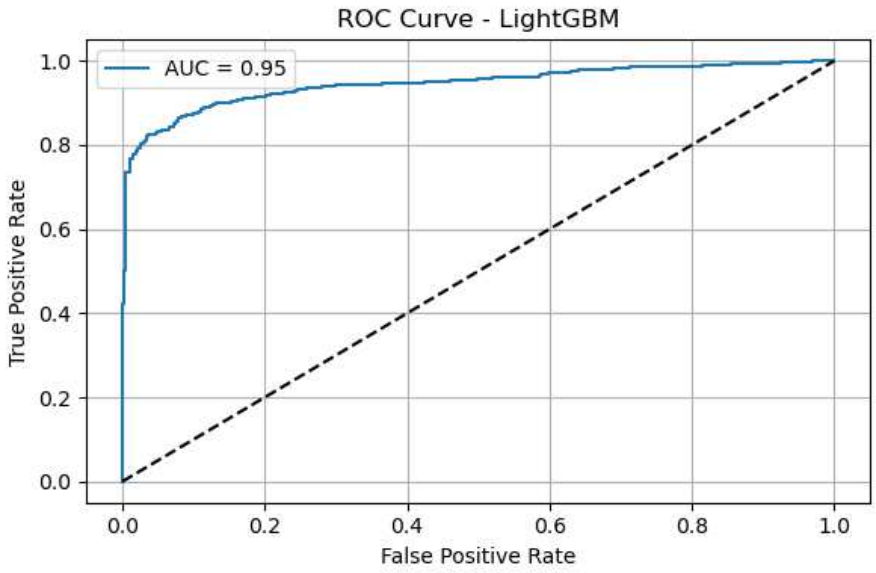


Fig. 4 ROC Curve for Spoof Detection

The precision-recall curve (Figure 5) confirms classifier effectiveness under imbalanced conditions, with precision remaining above 90% as recall approaches 1.0. This ensures the system rarely misses spoofed behaviors while minimizing false alarm rates.

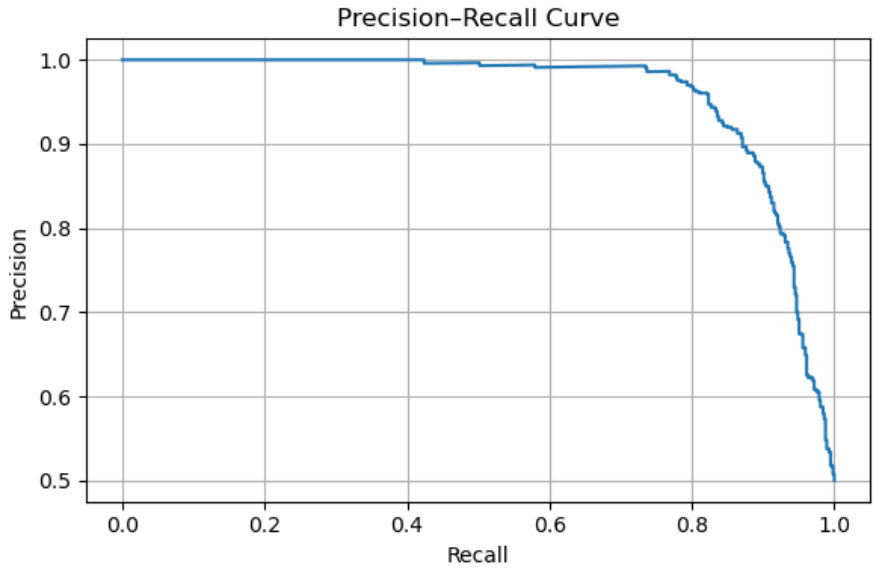


Fig. 5 Precision–Recall Curve

In wireless IoT setups, achieving high AUC and precision when data is unevenly distributed is very important. Spoofing detection needs to be sensitive to spot harmful Zigbee/Wi-Fi control actions, but it also needs to avoid giving too many false warnings.

4.4 Feature Importance and Explainability Analysis

Feature importance analysis (Figure 6) reveals the primary classification drivers:

- **Hour of Day**: Temporal context identifies unusual behavior outside typical operational windows
- **Rolling Mean Power**: Captures short-term stability patterns or erratic consumption behaviors
- **Power Efficiency**: Indicates anomalous energy usage relative to ambient environmental conditions

This analysis confirms the success of our feature engineering approach in capturing adversarial device behaviors rather than merely identifying raw signal outliers.

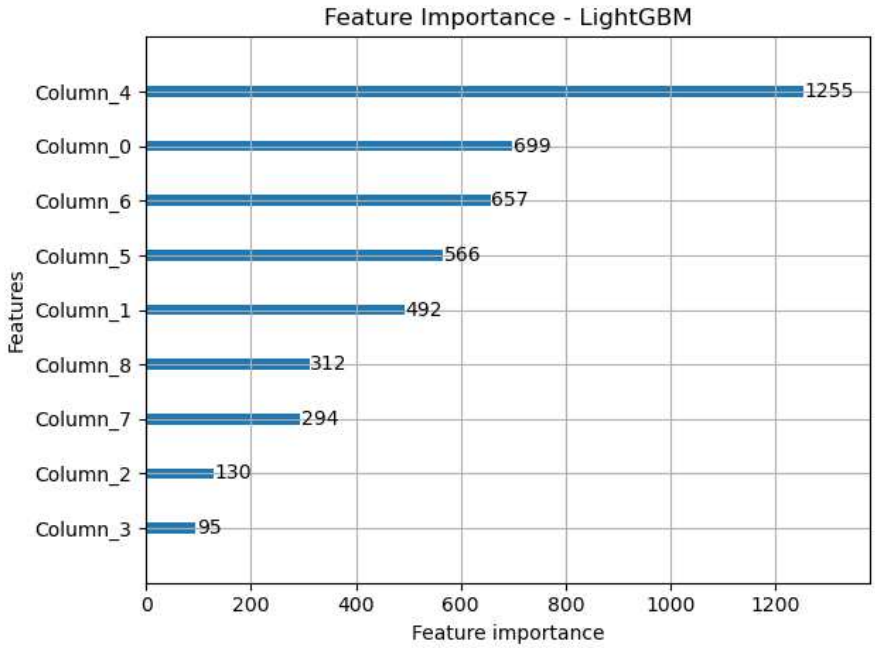


Fig. 6 Feature Importance Analysis (LightGBM)

These features may show misuse of wireless commands, such as unauthorized activation at odd times or power issues from bad control messages. This suggests they are important for wireless security across different layers.

4.5 Model Generalization and Learning Behavior

The learning curve analysis (Figure 7) demonstrates steady validation score improvement across increasing training set sizes, with narrowing gaps between training and validation performance. This indicates minimal overfitting and strong generalization capability—essential characteristics for real-world smart home systems where new device patterns or firmware updates may occur frequently.

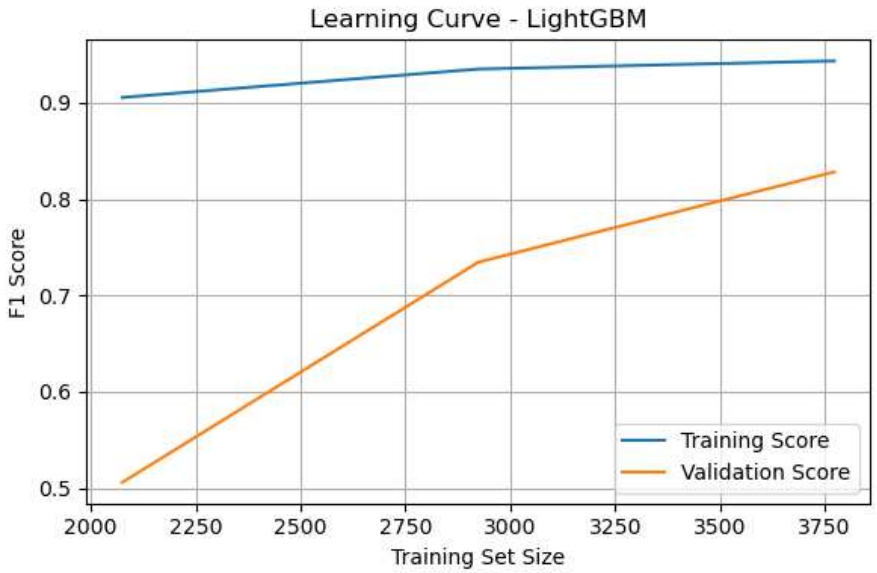


Fig. 7 Learning Curve of the Classifier

Consistent learning despite differing sample sizes indicates the system can withstand typical changes in wireless IoT setups, such as firmware revisions or the addition of new Zigbee/Wi-Fi devices.

4.6 Comprehensive Performance Metrics

The LightGBM classifier achieved robust performance across all key evaluation metrics:

- **Accuracy**: **90.00%**
- **F1 Score (macro)**: 0.8893
- **AUC Score**: 0.9464

Table 1 presents the complete classification report, highlighting balanced performance between normal and spoofed classes with consistent precision and recall metrics across both categories.

Table 1 Classification Performance Report

Class	Precision	Recall	F1-Score	Support
Normal (0)	0.85	0.95	0.90	566
Spoofed (1)	0.95	0.84	0.89	566
Accuracy		**0.90**		
Macro Avg	0.90	0.90	0.90	1132
Weighted Avg	0.90	0.90	0.90	1132

4.7 Discussion of Methodological Contributions and Security Implications

The core methodological contribution of this research lies in its systematic integration of adversarial behavior simulation with semantically grounded feature extraction. Unlike previous works that rely on fixed rule-based thresholds or generic anomaly detection approaches, our framework:

1. **Simulates realistic spoofing scenarios** aligned with physical plausibility constraints (e.g., elevated power consumption during idle operational states)
2. **Leverages domain-specific handcrafted features** that reflect the underlying behavioral logic of smart home environments
3. **Provides comprehensive explainability** through feature attribution analysis, supporting deployment in trust-critical security systems

For practical deployment, this methodology can be integrated into home gateways or cloud-based monitoring infrastructures. Given its computational efficiency and interpretability characteristics, the framework can provide early warning capabilities for device compromise, spoofing attempts, or remote hijacking incidents in smart home ecosystems and also this framework can be used with smart home gateways that connect to Zigbee/Wi-Fi devices. It acts as an added security layer to spot unusual behavior, working with existing wireless security measures that check for PHY/MAC anomalies.

5 Conclusion

This study presents a comprehensive framework for detecting adversarial spoofing behaviors in smart home environments through the integration of behavioral feature engineering, synthetic adversarial sample injection, and optimized LightGBM classification. Unlike previous approaches that rely heavily on labeled datasets or focus exclusively on network-level signals, our methodology leverages both cyber and physical behavioral indicators to construct a discriminative and interpretable feature space.

Through systematic spoofing injection and SMOTE-based data balancing, we demonstrate robust performance against class imbalance and adversarial behaviors. The classifier achieves 90% accuracy and an AUC of 0.9464, confirming its readiness

for real-world deployment scenarios. PCA visualization and feature importance analysis reveal that the model captures subtle behavioral differences that rule-based or unsupervised detectors often overlook.

Importantly, the proposed framework is computationally efficient, requires minimal labeled data, and provides comprehensive explainability, making it highly suitable for smart home applications where edge computing resources are limited and privacy preservation is paramount. The approach introduces a novel perspective for integrating behavioral modeling and adversarial reasoning into smart home intrusion detection systems.

This study looked at behavioral features. The signals come from IoT devices using Zigbee, Wi-Fi, and MQTT. Therefore, this is for wireless smart homes. The method models fake-caused behavioral problems, providing a simple way to spot them. It can be used on smart home gateways that handle wireless IoT traffic.

Future research will build on this by adding wireless data like RSSI drift, packet times, and PHY/MAC-level issues which will create a cross-layer detection setup. Also, using federated edge learning will allow several homes to work together while keeping data private. This is important for the future of wireless IoT. These steps will make it harder to do wireless spoofing, which supports the goals of Wireless Personal Communications.

6 Limitations and Future Work

While the proposed framework demonstrates strong accuracy and generalization capabilities for spoofed behavior detection in smart home systems, several limitations warrant further investigation and development.

First, the spoofed samples utilized in this study were synthetically generated using predefined heuristic rules. Although careful consideration was given to simulating realistic adversarial behaviors (e.g., elevated power consumption during inactive periods), these synthetic samples may not fully capture the diversity and sophistication of real-world spoofing attempts executed by advanced persistent threat actors. Future research should incorporate authentic spoofed activity traces or develop adversarial samples through generative modeling approaches or reinforcement learning-based attack simulation frameworks.

Second, the current implementation relies on a fixed feature set derived from domain expertise. While this design enhances interpretability and proves effective for known behavioral patterns, it may limit adaptability to previously unseen device types or emergent behavioral patterns in increasingly complex smart home configurations. Future work should explore automated feature discovery through neural architecture search methodologies or hybrid approaches combining handcrafted and learned representation techniques.

Third, the dataset employed reflects device behaviors under relatively static environmental and user contexts. Real-world smart home deployments typically experience dynamic changes including device firmware updates, evolving user routines, seasonal

variations, and contextual triggers (e.g., geolocation-based automation, holiday schedules). Evaluating model robustness under such temporal and contextual distribution shifts remains an important open challenge.

Additionally, while SMOTE was effectively employed to mitigate class imbalance issues, the synthetic nature of the oversampling approach may not adequately capture hard negative cases or borderline spoofing scenarios that exist at decision boundaries. Future investigations can explore advanced imbalance-handling methodologies such as dynamic sampling strategies, focal loss optimization, or semi-supervised anomaly scoring approaches.

Finally, although the current framework is designed for computational efficiency, validation has been conducted in offline batch processing mode. Deployment in real-time operational environments—such as home gateways or edge controllers—requires comprehensive latency profiling, streaming inference optimization, and on-device explainability capabilities, which are crucial for practical adoption in production smart home systems.

Future research directions include extending the architectural foundation with contrastive self-supervised learning to effectively handle unlabeled data streams, integrating federated learning paradigms for privacy-preserving multi-home collaborative detection, and simulating coordinated multi-device spoofing scenarios and protocol-layer attacks to evaluate defensive capabilities against more sophisticated threat models.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations

Clinical Trial Registration

Not applicable.

Consent to Participate

Not applicable.

Consent to Publish

Not applicable.

Ethics Approval

Not applicable.

References

[1] D. H. Tran, V. L. Nguyen, H. Nguyen, and Y. M. Jang, "Self-supervised learning for time-series anomaly detection in industrial internet of things," *Electronics*, vol. 11, no. 14, p. 2146, 2022.

[2] H. Qiu *et al.*, "Adversarial attacks against network intrusion detection in IoT systems," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10327–10341, Jul. 2021.

[3] Y. Ibrahim and S. Ambareen, "Avoiding occupancy detection from smart meter using adversarial machine learning," *IEEE Access*, vol. 9, pp. 35411–35430, 2021.

[4] S. H. Rafique *et al.*, "Machine learning and deep learning techniques for IoT network anomaly detection—Current trends," *Sensors*, vol. 24, no. 6, p. 1968, 2024.

[5] Elsas, R., Van Leemput, D., Hoebeke, J., et al. (2023). Multi-Modal Industrial IoT Networks: Recent Advances and Future Challenges. Wireless Personal Communications, 140, 1–24.

[6] P. Zhang and S. G. Nagarajan, "SAD-IoT: Security Analysis of DDoS Attacks in IoT Networks," *Wireless Personal Communications*, vol. 122, no. 1, pp. 87–108, 2022, doi:10.1007/s11277-021-08890-6.

[7] E. Gelenbe, M. Nakıp, and M. Siavvas, "Online self-supervised deep learning for intrusion detection systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 5668–5683, 2024.

[8] T. D. Nguyen *et al.*, "DÏoT: A federated self-learning anomaly detection system for IoT," in *Proc. ACM WiSec*, 2018, pp. 195–206.

[9] M. A. Ferrag *et al.*, "Anomaly detection and classification for smart home networks using LSTM," *Appl. Soft Comput.*, vol. 113, p. 107889, 2021.

[10] S. Deldari *et al.*, "COCOA: Cross-modality contrastive learning for sensor data," *Sensors*, vol. 22, no. 15, p. 5732, 2022.

[11] E. Eldele *et al.*, "TS-TCC: Temporal and contextual contrasting for self-supervised time-series representation learning," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 9, pp. 5543–5558, Sep. 2022.

[12] X. Wang *et al.*, "A CNN-based anomaly detection model for smart home IoT systems," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2650–2660, Feb. 2022.

[13] Y. Zhang, P. Alahakoon, and D. Lin, "Smart home intrusion detection via graph neural networks with multimodal sensor data," *Ad Hoc Netw.*, vol. 164, p. 103598, 2023.

[14] H. Farrukh and R. Sommer, "Evasion attacks and defenses on smart home physical event sensors," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10567–10580, Jun. 2022.

[15] Y. Li *et al.*, "Self-supervised learning for smart home IoT anomaly detection," *Pattern Recognit. Lett.*, vol. 162, pp. 29–36, 2023.

[16] Z. Raza *et al.*, "Adversarial attacks on ML-based IoT anomaly detection systems," *Comput. Netw.*, vol. 208, p. 108845, 2022.

[17] M. Rahman and A. Hussain, "Lightweight intrusion detection for IoT: A survey," *Comput. Commun.*, vol. 148, pp. 180–200, 2020.

[18] X. Zhou *et al.*, "A contrastive learning approach for enhanced robustness in federated edge intelligence," *Ad Hoc Netw.*, vol. 140, p. 103245, 2024.

[19] M. Tantawy, "Anomaly detection based on artificial intelligence of things (AIoT)," *Comput. Intell. Neurosci.*, vol. 2023, Art. no. 3451245, 2023.

[20] M. R. Shahid *et al.*, "Anomalous communications detection in IoT networks using sparse autoencoders," *Comput. Netw.*, vol. 162, p. 106857, 2019.

[21] L. Zhang, Y. Wang, and X. Liu, "Machine learning approaches for IoT device classification: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1238–1265, 2021.

[22] Y. Meidan *et al.*, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018.

[23] IEEE DataPort, "Smart Home Device Behavior Dataset," [Online]. Available: https://ieee-dataport.org/documents/smarthomedevicedataset