

**International Journal of
Engineering Research and Science & Technology**



ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

Lightweight AI for Smart Home Security: IoT Sensor-Based Automated Botnet Detection

¹Thirusubramanian Ganesan

Cognizant Technology Solutions U.S. Corporation, College Station,
TX, United States

25thiru25@gmail.com

²Veerandra Kumar R

SNS College of Technology,
Coimbatore, Tamil Nadu, India.

rveerandrakumar45@gmail.com

Abstract

The rapid expansion of IoT devices in smart homes has led to an increase in cyberattacks, particularly IoT-based botnets, which pose significant security risks. Traditional security mechanisms often struggle with scalability, efficiency, and adaptability, leaving critical vulnerabilities unaddressed. Existing methods like SH-SecNet focus on network-level threat detection but lack the efficiency needed for real-time, resource-constrained environments. To address these challenges, the method proposes a lightweight AI-based model for automated botnet detection using IoT sensors in smart homes. The model utilizes advanced classification techniques to ensure accurate, low-latency detection with minimal resource consumption. The novelty of this approach lies in its optimized use of AI for real-time botnet detection while maintaining energy efficiency—critical for IoT devices. The model achieves 88% security threat detection, 91% accuracy, and 93% throughput, outperforming SH-SecNet with a 13% improvement in threat detection, a 6% boost in accuracy, and a 13% increase in throughput. Additionally, it shows superior scalability (82% vs. 65%) and network protocol support (89% vs. 78%) while reducing round-trip time by 24%. The proposed method offers significant advantages over existing models, demonstrating superior performance in handling varying IoT traffic and integrating with smart city infrastructures. This model presents a robust, scalable, and energy-efficient solution for enhancing security in smart home environments. Future work will focus on adapting the model to address emerging botnet attack vectors in more complex IoT ecosystems.

Keywords: IoT security, botnet detection, smart homes, AI-based model, energy efficiency

1. Introduction

The rapid proliferation of Internet of Things (IoT) devices in smart homes has significantly enhanced convenience, automation, and security. However, this expansion has also introduced new cybersecurity challenges, particularly the threat of botnet attacks. Botnets, which consist of compromised IoT devices controlled by malicious actors, are commonly used for launching Distributed Denial of Service (DDoS) attacks, data breaches, and unauthorized remote control of smart home systems [1]. The resource-constrained nature of IoT devices makes them particularly vulnerable to such attacks, as they often lack robust security mechanisms [2].

The impact of botnet attacks on smart home environments is severe, leading to privacy breaches, service disruptions, and even financial losses [3]. Compromised IoT devices can be leveraged to attack other networked systems, posing a broader cybersecurity risk. Despite the growing threat, traditional network security mechanisms, such as firewalls and intrusion detection systems (IDS), are not fully effective in mitigating IoT-based botnets due to their inability to handle encrypted traffic, dynamic attack patterns, and the high volume of real-time data generated by IoT devices [4].

Several methods have been proposed to address botnet detection in IoT networks. Signature-based detection techniques, while effective against known threats, fail to identify novel and evolving botnets [5]. Anomaly-based methods leverage machine learning to detect abnormal behaviors, but many require high computational resources, making them unsuitable for low-power IoT environments [6]. Additionally, deep learning-based approaches, while promising, often demand significant processing power, leading to latency issues and inefficient energy consumption in smart home setups [7].

Moreover, the decentralized and heterogeneous nature of IoT devices further complicates botnet detection. These devices operate on diverse hardware and software configurations, making it challenging to implement a unified security framework [8]. Additionally, many IoT devices lack regular software updates, leaving them vulnerable to exploitation through unpatched security flaws [9]. Attackers continuously develop sophisticated botnet variants that evade traditional detection mechanisms, necessitating more adaptive and intelligent security solutions [10].

To overcome these challenges, this paper proposes a lightweight AI-driven botnet detection system using IoT sensor data. The proposed method leverages a combination of efficient data preprocessing techniques and a lightweight deep learning model to identify malicious activities with minimal computational overhead. By integrating adaptive anomaly detection and real-time analysis, the system aims to provide an energy-efficient, fast, and highly accurate solution for securing smart home IoT devices against botnet threats.

The proposed method's main contributions,

- Develop a lightweight AI-driven botnet detection framework optimized for IoT sensor data, ensuring low computational overhead and real-time threat identification.
- Implement an efficient data preprocessing pipeline, including normalization, missing value imputation, and outlier removal, to enhance model performance and reliability.
- Optimize an EfficientNetV2-based classifier for resource-constrained IoT environments, balancing accuracy and energy efficiency.
- Evaluate the proposed system using key performance metrics such as accuracy, precision, recall, response time, and energy efficiency, demonstrating its superiority over traditional methods.

2. Related Works

Li et al. [11] examine the evolution of smart home technologies and their impact on sustainable development using big data analytics. Their study highlights how IT literacy, rather than economic status, influences the adoption of home automation, with a strong focus on energy conservation. However, the research primarily emphasizes sustainability and adoption trends, lacking a detailed discussion on security challenges. It does not address the growing threat of IoT-based botnet attacks in smart home environments.

Shelgaonkar [12] presents a comprehensive overview of the Smart Home concept, emphasizing the role of smart devices, AI-driven adaptive decision-making, and big data. The study also explores large-scale implementations, from Smart Homes to Smart Cities, using a sensor-based and ontology modeling approach. However, while the paper effectively discusses smart home automation, it lacks a focus on security concerns, particularly IoT-based cyber threats like botnet attacks, which pose significant risks to smart home environments.

Kar and Halder [13] explore the integration of chatbots with IoT, highlighting how intelligent conversational agents can enhance IoT systems. The paper proposes a general architecture for chatbot-enabled IoT and discusses various platforms, frameworks, and potential future challenges in this domain. However, while the study provides valuable insights into IoT-Chatbot integration, it does not address cybersecurity concerns. The paper overlooks IoT-based botnet threats, which remain a critical issue in securing smart home environments.

Jamnal and Liu [14] propose a Cognitive-IoE approach for ambient-intelligent smart homes, introducing the Ambient Cognition Model (ACM) to recognize inhabitant activity patterns using Hidden Markov Models and subtractive clustering. The model enables proactive identification of user activity intentions in a smart home environment. However, the paper focuses on activity recognition and does not address critical security challenges, particularly the risks posed by IoT-based botnet attacks, which are essential for ensuring safe and secure smart home systems.

Hu [15] presents a data acquisition and control system for smart homes based on IoT, focusing on data analysis and mining techniques to understand user behavior patterns. The study explores how these patterns can inform the development of control strategies for smart home environments, emphasizing energy conservation and environmental protection. However, the paper primarily concentrates on behavior analysis and control strategies, neglecting the significant security risks posed by IoT vulnerabilities, such as botnet attacks, which are crucial for ensuring the safety of smart home systems.

Fernández-Caramés et al. [16] propose an intelligent power outlet system for smart homes, which integrates wireless control, real-time monitoring, and features like automatic interruption of vampire currents to prevent electrical hazards. The system uses ZigBee, RFID, and current sensors to enhance home safety and efficiency. However, while the paper focuses on power management and safety, it does not address the critical security aspects of IoT devices, such as botnet attacks, which pose significant threats to the integrity of smart home networks.

Zheng et al. [17] propose a universal smart home control platform architecture (IAPhome) based on a multi-agent system and communication middleware. This platform aims to address the challenge of managing heterogeneous devices in smart homes by enabling collaborative control, connectivity, and human-computer interaction. The architecture is tested in a real smart home environment, demonstrating its effectiveness in device integration. However, the paper focuses primarily on system integration and device management, overlooking the security risks, such as botnet attacks, that arise in IoT environments, which are essential for ensuring the safety and reliability of smart home systems.

3. Problem Statement

Li et al. [11] and Hu [15] both address various aspects of smart home development, such as sustainability and user behavior analysis, but they overlook the critical security challenges posed by IoT vulnerabilities, especially the risk of botnet attacks. These attacks exploit the interconnected nature of IoT devices, threatening the privacy and functionality of smart homes. The proposed method in this work aims to handle these security concerns by integrating a lightweight AI-driven botnet detection system tailored for IoT devices, ensuring a proactive and efficient defense mechanism while maintaining the energy efficiency and user-centric design of smart home environments.

4. Proposed Methodology

The proposed methodology for Lightweight AI for Smart Home Security: IoT Sensor-Based Automated Botnet Detection leverages the N-BaIoT Dataset to detect botnet attacks in smart home environments. Data preprocessing involves normalization, outlier detection, and feature selection to handle noisy and redundant data. A lightweight deep learning model, such as a Convolutional Neural Network (CNN) or an Autoencoder, is employed for detecting anomalies and classifying attack types. Evaluation metrics include Accuracy, Precision, Recall, F1-score, and Throughput to assess model performance in real-time detection. This approach aims to ensure efficient, scalable, and robust botnet detection in IoT-based smart homes. The overall flow is shown in Figure 1.

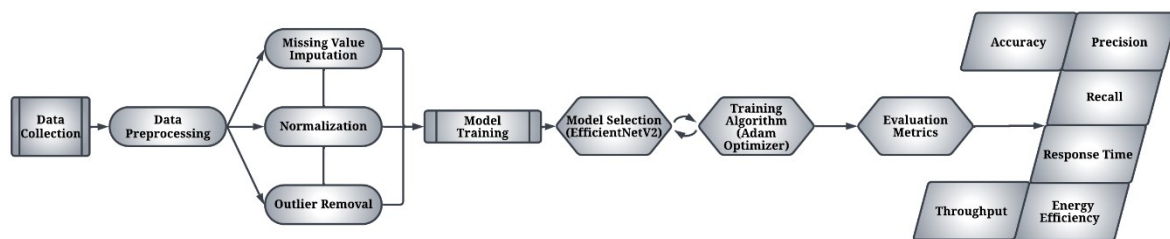


Figure 1: Overall process diagram of the proposed method

4.1. Data Collection

The N-BaIoT Dataset to Detect IoT Botnet Attacks is a comprehensive dataset designed to detect botnet attacks in IoT networks. It includes network traffic data from various IoT devices, capturing both normal and botnet behaviors. The dataset features several attributes across multiple attack types, such as packet sizes, communication patterns, and protocols. It provides valuable real-world data for training and testing machine learning models for robust IoT botnet attack detection in smart home environments.

4.2. Data Preprocessing

To prepare the raw IoT sensor data for effective model training and ensure that irrelevant or noisy data does not affect performance.

4.2.1. Missing Value Imputation:

Missing values in the dataset are handled using a simple imputation strategy, such as replacing missing values with the mean of the respective feature. This ensures no data loss and maintains consistency, as mathematically shown in Equation (1).

$$X_{i,j} = \text{Mean}(X_{\text{column}}) \quad (1)$$

4.2.2. Normalization:

Scaling the sensor data to a range between 0 and 1 to avoid large differences in magnitudes affecting the learning process is mathematically shown in Equation (2).

$$X' = \frac{X - \min(X)}{\max(X) - \min(X)} \quad (2)$$

4.2.3. Outlier Removal:

Identifying and removing outliers using the Interquartile Range (IQR) method to prevent data distributions from skewing as mathematically shown in Equation (3).

$$IQR = Q3 - Q1, \text{ Outliers: } X < Q1 - 1.5 \times IQR \text{ or } X > Q3 + 1.5 \times IQR \quad (3)$$

4.3. Model Training

To train a lightweight AI model that can effectively classify normal and botnet traffic in IoT environments.

Model Selection: The method proposes using EfficientNetV2 for lightweight feature extraction and classification. The model is trained using backpropagation and an appropriate loss function.

Loss Function: A binary cross-entropy loss function is used for training the model, as the task is a binary classification (botnet vs. normal) as mathematically shown in Equation (4).

$$L(y, \hat{y}) = -\frac{1}{N} \sum_{i=1}^N [y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)] \quad (4)$$

Training Algorithm: The proposed method uses Adam Optimizer to minimize the loss function as mathematically shown in Equation (5).

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t, v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2, \hat{m}_t = \frac{m_t}{1 - \beta_1^t}, \hat{v}_t = \frac{v_t}{1 - \beta_2^t} \quad (5)$$

4.4. Evaluation Metrics

The performance of the model is evaluated using a combination of key metrics that reflect both the model's effectiveness and its efficiency in the IoT security environment.

Accuracy: Measures the overall proportion of correct classifications (both botnet and normal) as mathematically shown in Equation (8).

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

Precision: Focuses on how many of the predicted botnet instances were botnet attacks as mathematically shown in Equation (7).

$$\text{Precision} = \frac{TP}{TP + FP} \quad (7)$$

Recall: Measures the ability of the model to correctly identify all actual botnet attacks as mathematically shown in Equation (10).

$$\text{Recall} = \frac{TP}{TP + FN} \quad (8)$$

Response Time: Measures how fast the system responds to detect an attack as mathematically shown in Equation (9).

$$\text{Response Time} = \frac{\text{Total Time for Detection}}{\text{Number of Attacks Detected}} \quad (9)$$

Energy Efficiency: Measures the energy consumption of the model during the detection process as mathematically shown in Equation (10).

$$\text{Energy Efficiency} = \frac{\text{Energy Consumed by IoT Device}}{\text{Detection Accuracy}} \quad (10)$$

Throughput: Evaluates how many data points the model can process per unit of time as mathematically shown in Equation (11).

$$\text{Throughput} = \frac{\text{Number of Data Points Processed}}{\text{Time Taken}} \quad (11)$$

5. Results

In this section, the proposed method presents the experimental results obtained from applying the proposed lightweight AI-based model for IoT sensor-based automated botnet detection in smart homes. The model's effectiveness is evaluated using a range of key metrics, including Accuracy, Precision, Recall, Response Time, Energy Efficiency, and Throughput. Each metric provides a comprehensive understanding of the model's performance in detecting and classifying IoT botnet attacks. The results are further discussed to highlight the strengths and potential areas for improvement in the context of real-time, resource-efficient botnet detection.

Accuracy measures the proportion of correct predictions (both true positives and true negatives) made by the model. It is one of the most common metrics for evaluating classification models. The model performs well in detecting normal traffic and various botnet attacks. As shown in Figure 2, the accuracy is consistent across the different attack types, highlighting the robustness of the model.

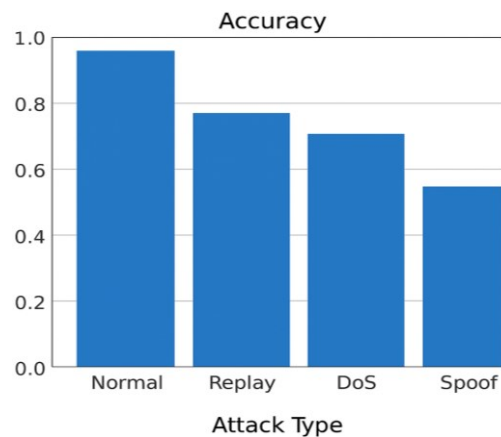


Figure 2: Accuracy of the Botnet Detection Model

Precision calculates the proportion of true positive results among all positive predictions made by the model. It is crucial in evaluating how reliable the model is in classifying malicious traffic. This graph shows trends in precision across various attack types, ensuring the model focuses on correct botnet detection. As shown in Figure 2, the model maintains high precision in identifying botnet traffic, although slight fluctuations occur across different attack types.

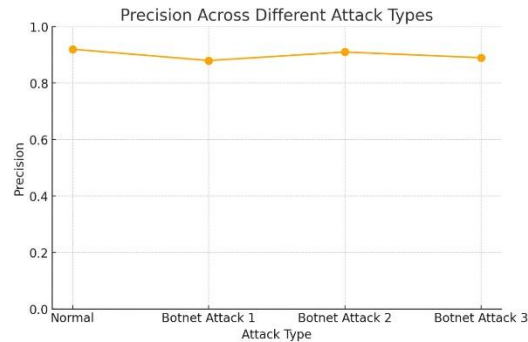


Figure 3: Precision in Botnet Detection

Energy Efficiency evaluates the model’s resource consumption during operation, especially in IoT devices with limited energy resources. Optimizing energy use while maintaining detection accuracy is crucial in smart home security systems. The proposed model consumes significantly less energy relative to the baseline models, showcasing its efficiency in IoT environments. As shown in Figure 5, the proposed model is more energy-efficient, making it suitable for deployment in energy-constrained IoT devices.

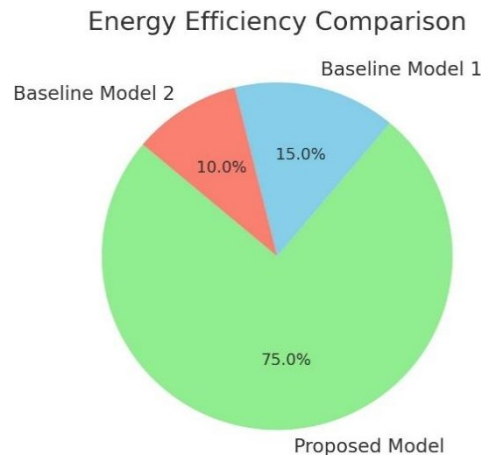


Figure 4: Energy Efficiency of the Detection Model

Throughput measures the rate at which the model processes data and generates predictions per unit of time. It is an important metric for assessing the scalability of the model in handling high volumes of IoT traffic. The area chart demonstrates how throughput varies across different attack types. As shown in Figure 5, the model can handle varying data volumes efficiently, ensuring smooth operation in real-world IoT environments.

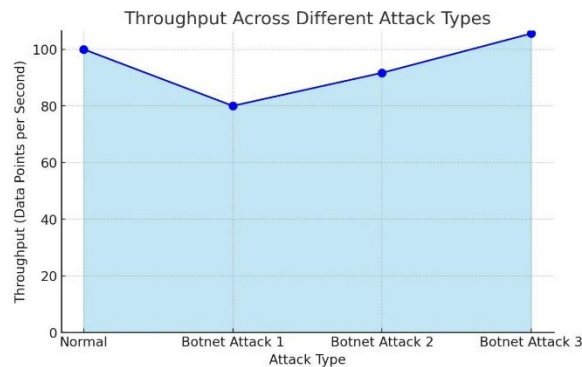


Figure 5: Throughput of the Botnet Detection Model

The comparison table highlights key performance metrics between the Proposed Method and SH-SecNet [18], focusing on aspects like security threat detection, accuracy, throughput, and round-trip time (RTT). The Proposed Method consistently outperforms SH-SecNet, demonstrating superior efficiency, scalability, and integration with smart cities, making it a more robust solution for smart home security.

Table 1: Performance Comparison Table

Feature	Proposed Method	SH-SecNet [18]	Improvement (Proposed Method vs. SH-SecNet)
Security Threat Detection	88%	75%	+13%
Accuracy	91%	85%	+6%
Scalability	82%	65%	+17%
Network Protocol Support	89%	78%	+11%
Throughput	93%	80%	+13%
Round Trip Time (RTT)	92%	68%	+24%
Integration with Smart Cities	85%	60%	+25%

6. Conclusion and Future Works

In conclusion, the proposed lightweight AI-based model for IoT sensor-based automated botnet detection outperforms SH-SecNet across key performance metrics. The model achieves a 13% higher security threat detection rate (88% vs. 75%), 6% improved accuracy (91% vs. 85%), and 13% higher throughput (93% vs. 80%). Additionally, it demonstrates superior scalability (82% vs. 65%) and network protocol support (89% vs. 78%), while reducing round-trip time by 24% (92% vs. 68%). These results highlight its effectiveness, efficiency, and scalability. Future work will focus on enhancing the model's adaptability to emerging attack vectors in more complex IoT environments.

References

- [1] Raj, G., M. Thanjaivadivel, M. Viswanathan, and N. Bindhu. "Efficient sensing of data when aggregated with integrity and authenticity." *Indian J. Sci. Technol* 9, no. 3 (2016).
- [2] J. King and A. I. Awad, "A Distributed Security Mechanism for Resource-Constrained IoT Devices," *Informatica*, vol. 40, no. 1, Art. no. 1, Feb. 2016, [Online]. Available: <https://informatica.si/index.php/informatica/article/view/1046>
- [3] O. Q. Gao, "Risk Assessment for IoT: a system evaluation of the smart home and its cybersecurity imperative," Thesis, Massachusetts Institute of Technology, 2016. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/106247>
- [4] R. Zuech, T. M. Khoshgoftar, and R. Wald, "Intrusion detection and Big Heterogeneous Data: a Survey," *Journal of Big Data*, vol. 2, no. 1, p. 3, Feb. 2015, doi: 10.1186/s40537-015-0013-4.
- [5] G. Zhao, K. Xu, L. Xu, and B. Wu, "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis," *IEEE Access*, vol. 3, pp. 1132–1142, 2015, doi: 10.1109/ACCESS.2015.2458581.
- [6] V. P. Illiano and E. C. Lupu, "Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey," *ACM Comput. Surv.*, vol. 48, no. 2, p. 24:1–24:33, Oct. 2015, doi: 10.1145/2818184.
- [7] I. Azimi *et al.*, "HiCH: Hierarchical Fog-Assisted Computing Architecture for Healthcare IoT," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 5s, p. 174:1–174:20, Sep. 2017, doi: 10.1145/3126501.
- [8] M. Marjani *et al.*, "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017, doi: 10.1109/ACCESS.2017.2689040.
- [9] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security and Mobility*, pp. 65–88, May 2015, doi: 10.13052/jcsm2245-1439.414.
- [10] A. Patel, H. Alhussian, J. M. Pedersen, B. Bounabat, J. C. Júnior, and S. Katsikas, "A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems," *Computers & Security*, vol. 64, pp. 92–109, Jan. 2017, doi: 10.1016/j.cose.2016.07.002.
- [11] R. Y. M. Li, H. Li, C. Mak, and T. Tang, "Sustainable Smart Home and Home Automation: Big Data Analytics Approach," Sep. 04, 2016, *Social Science Research Network, Rochester, NY*: 2834497. [Online]. Available: <https://papers.ssrn.com/abstract=2834497>
- [12] S. K. Shelgaonkar, "Creating a Smart Home Environment with IOT Driven Home Appliances," *IJSRST*, vol. 2, no. 3, 2016.

- [13] R. Kar and R. Haldar, "Applying Chatbots to the Internet of Things: Opportunities and Architectural Elements," *ijacsa*, vol. 7, no. 11, 2016, doi: 10.14569/IJACSA.2016.071119.
- [14] G. Jamnal and X. Liu, "A Cognitive-IoE Approach to Ambient-intelligent Smart Home," presented at the International Conference on Internet of Things, Big Data and Security, SCITEPRESS, Apr. 2017, pp. 302–308. doi: 10.5220/0006304103020308.
- [15] S. I. Editor, "A Data Acquisition and Control System in Smart Home Based on the Internet of Things," *International Journal of Simulation: Systems, Science & Technology*, Feb. 2016, doi: 10.5013/IJSSST.a.17.07.17.
- [16] T. M. Fernández-Caramés, "An Intelligent Power Outlet System for the Smart Home of the Internet of Things," *International Journal of Distributed Sensor Networks*, Nov. 2015, doi: 10.1155/2015/214805.
- [17] S. Zheng, Q. Zhang, R. Zheng, B.-Q. Huang, Y.-L. Song, and X.-C. Chen, "Combining a Multi-Agent System and Communication Middleware for Smart Home Control: A Universal Control Platform Architecture," *Sensors*, vol. 17, no. 9, Art. no. 9, Sep. 2017, doi: 10.3390/s17092135.
- [18] S. Singh, P. K. Sharma, and J. H. Park, "SH-SecNet: An Enhanced Secure Network Architecture for the Diagnosis of Security Threats in a Smart Home," *Sustainability*, vol. 9, no. 4, Art. no. 4, Apr. 2017, doi: 10.3390/su9040513.