International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI-Driven Anomaly Detection for IoT Devices in Smart Homes using Android-Based Mobile Applications

Vijay Kumar Meena

Lecturer,Govt. Rajesh Pilot Polytechnic College,Dausa

Email:-vijaysattawan22@gmail.com

Submitted: 14/06/2018 **Revised:** 20/07/2018 **Accepted:** 10/08/2018

Abstract: The increasing adoption of Internet of Things (IoT) devices in smart homes has transformed daily living through enhanced automation, remote access, and energy optimization. However, these devices introduce vulnerabilities due to limited computational resources, heterogeneous communication protocols, and weak authentication mechanisms. Traditional security approaches, including signature-based intrusion detection systems, are insufficient to address modern cyber threats such as zero-day attacks, botnet infiltration, and data exfiltration. This paper proposes an **AI-driven anomaly detection framework** that leverages a **hybrid Long Short-Term Memory (LSTM) and Random Forest (RF) model** for real-time anomaly detection in IoT ecosystems. The framework is integrated into an **Android-based mobile application** that provides end-users with anomaly alerts, visualization dashboards, and device isolation controls. The system is evaluated using the **TON_IoT dataset**, achieving an accuracy of **96.8%**, precision of **95.2%**, and recall of **94.6%**, outperforming traditional machine learning baselines. A usability study with **30 participants** confirmed high user satisfaction, scoring an average of **4.6/5** in usability. This work demonstrates the feasibility of combining advanced AI models with mobile interfaces to enhance smart home IoT security, while addressing issues of latency, accessibility, and user experience.

Keywords: IoT Security, Smart Homes, Anomaly Detection, Artificial Intelligence, Mobile Application, Android.

I. Introduction

A. Background and Motivation

The concept of the **smart home** is increasingly becoming a reality due to the rapid adoption of **Internet of Things (IoT)** devices. These devices enable automation in areas such as lighting, heating, entertainment systems, security monitoring, and household appliances. According to market research, the global smart home market is projected to reach over **USD 200 billion by 2026** [1].

While smart homes enhance **convenience, energy efficiency, and accessibility**, they also introduce significant **security challenges**. IoT devices are characterized by their **resource-constrained hardware, lack of standardized protocols, and frequent exposure to external networks**, which make them highly vulnerable to cyberattacks [2]. Well-documented IoT attacks such as **Mirai botnet** and **BrickerBot** have demonstrated the devastating potential of compromised IoT ecosystems [3].

B. Problem Statement

Traditional **signature-based intrusion detection systems (IDS)** are ineffective against unknown or evolving threats. Furthermore, most anomaly detection systems require **powerful computational resources**, making them unsuitable for deployment on lightweight IoT devices [4]. Cloud-based anomaly detection introduces additional **latency** and **privacy risks** due to dependence on third-party services [5].

This creates a pressing need for an **edge-enabled anomaly detection system** that is:

1. **Lightweight enough** to integrate with smart home ecosystems.
2. **Intelligent enough** to detect novel anomalies.
3. **Accessible enough** to provide real-time alerts through a user-friendly platform.

C. Proposed Solution

This paper introduces a **hybrid anomaly detection system** based on **AI models (LSTM + Random Forest)**, embedded into an **Android-based mobile application**.

The system monitors IoT traffic, detects anomalous behavior in real-time, and provides actionable alerts to users. Unlike prior approaches, it bridges the gap between **state-of-the-art anomaly detection algorithms** and **consumer-level mobile applications**, ensuring that smart homeowners can directly benefit from advanced IoT security.

II. Related Work

A. Signature-Based Detection

Signature-based IDS rely on **predefined attack patterns** to identify malicious activity. While effective for known attacks, they **fail to detect zero-day exploits and polymorphic attacks** (Meidan et al., 2017) [6].

B. Machine Learning Approaches

Machine learning (ML) models such as **Support Vector Machines (SVM), Decision Trees, and Random Forests** have been widely used in IoT anomaly detection [7]. These models can generalize beyond signature-based systems but often struggle with **imbalanced datasets** and **real-time scalability**.

C. Deep Learning Approaches

Deep learning methods, particularly **Convolutional Neural Networks (CNNs)** and **Long Short-Term Memory (LSTM) networks**, have demonstrated high accuracy in IoT anomaly detection tasks [8]. However, they demand significant computational power, making deployment on IoT devices impractical.

D. Mobile Security Applications

Existing mobile applications for IoT security mainly focus on **device management, authentication, and firewall controls**, with **limited integration of AI-based anomaly detection**. Thus, there remains a gap between **advanced research models** and **consumer-usable applications**.

III. Methodology

A. System Architecture

The proposed framework consists of three primary layers:

1. **IoT Data Collection Layer**
   - Captures telemetry, system logs, and packet-level traffic from IoT devices.
   - Data features include packet size, protocol type, source/destination IP, timestamps, and device ID.
2. **AI-Driven Anomaly Detection Engine**
   - **LSTM model** analyzes sequential dependencies in IoT traffic.
   - **Random Forest classifier** categorizes anomalous events into attack types.
   - A hybrid ensemble of both models improves generalization.
3. **Android Mobile Application**
   - User-facing component built with **Java + Android Studio**.
   - Provides real-time anomaly alerts, dashboards, and remote device isolation features.

B. Dataset and Preprocessing

The **TON_IoT dataset** [1], comprising telemetry and network traces under normal and attack scenarios, was used. Data preprocessing included:

- **Normalization** of features.
- **Feature extraction** (e.g., frequency of packets, protocol types).
- **Train-test split** (70%-15%-15%).

C. Model Training

- **LSTM:** Trained for 50 epochs, batch size of 64, learning rate = 0.001.
- **Random Forest:** 200 decision trees, max depth = 15.
- **Hybrid:** Combines LSTM outputs as features for RF classification.

D. Android Application Development

- Developed in **Java (Android Studio)**.
- Backend: **Firebase Realtime Database** for storing anomalies and alerts.
- Features:
  - Dashboard for device activity visualization.
  - Push notifications for anomalies.
  - Device isolation commands.

IV. Results

A. Model Performance

Table I: Model Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	87.5%	85.2%	83.9%	84.5%
Random Forest	92.3%	90.7%	89.6%	90.1%
LSTM	94.1%	92.8%	92.0%	92.4%
Hybrid (LSTM + RF)	**96.8%**	**95.2%**	**94.6%**	**94.9%**

B. Application Usability

Table II: Android App Usability Scores (n=30 participants)

Parameter	Mean Score (1–5)
Ease of Use	4.6
Real-Time Responsiveness	4.7
Alert Effectiveness	4.5
Visualization Clarity	4.3
Overall Satisfaction	4.6

C. System Latency

The anomaly detection latency was measured at **320 ms**, confirming suitability for **real-time monitoring**.

V. Discussion

A. Comparison with Existing Approaches

- Signature-based IDS detect only known threats [6].
- Traditional ML models show moderate accuracy but lack temporal awareness [7].
- Deep learning models achieve high accuracy but require heavy computation [8].
- The proposed hybrid model combines **temporal pattern recognition (LSTM)** with **robust classification (RF)**, achieving higher detection rates with reduced false positives.

B. Mobile Application Benefits

Unlike purely cloud-based systems, this Android app ensures:

- **Accessibility:** Direct alerts to homeowners.
- **Low latency:** Local anomaly detection reduces cloud dependency.
- **User empowerment:** Enables isolation of compromised devices.

C. Challenges and Limitations

- **Scalability:** Handling data from **hundreds of IoT devices** may require distributed architectures.
- **Privacy:** Transmission of telemetry data introduces risks.
- **Energy consumption:** Continuous monitoring may drain mobile device battery.

VI. Conclusion and Future Work

This paper presents an **AI-driven anomaly detection framework** integrated into an **Android-based mobile application** for smart home IoT security. By leveraging a hybrid **LSTM + RF model**, the system achieved **96.8% accuracy** and real-time anomaly alerts with **high user satisfaction**.

Future work includes:

1. **Federated learning** to enable decentralized anomaly detection.
2. **Blockchain integration** for immutable device logs.
3. **Cross-domain deployment** across healthcare IoT and industrial IoT.

References

[1] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42.

[2] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27.

[3] Banos, O., Damas, M., Pomares, H., Rojas, I., Delgado-Marquez, B., & Valenzuela, O. (2014). Human activity recognition based on a sensor weighting hierarchical classifier. Soft Computing, 17(2), 333–343.

[4] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303–336.

[5] Chen, J., & Chen, Y. (2018). Smart home security: Challenges and solutions. IEEE Communications Magazine, 56(1), 28–34.

[6] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

[7] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. IEEE Security and Privacy Workshops, 29–35.

[8] Dua, S., & Du, X. (Eds.) (2016). Data Mining and Machine Learning in Cybersecurity. Boca Raton, FL: CRC Press.

[9] Jiang, J., Chen, J., Yu, H., Liu, Y., & Liu, R. (2017). Anomaly detection for IoT time-series data based on deep learning. IEEE International Conference on Data Mining Workshops (ICDMW).

[10] Khan, M. A., Salah, K., & Rehman, M. H. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.

[11] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84.

[12] Liu, H., Lang, B., Liu, M., & Yan, H. (2016). CNN and RNN based payload classification methods for attack detection. Knowledge-Based Systems, 108, 56–66.