WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

SmartGuard: Detecting Odd Behavior in IoT Devices Using Machine Learning

Juluru Chaitanya Sai[1],K Manikanta[2],R Thulchi Ram[3],Keerthi Chendra Gouni[4]

Kiran.kalvacherla2@gmial.com,
Ace Engineering College

ABSTRACT :

SmartGuard introduces a powerful, ML-based framework designed to detect abnormal behavior in IoT devices in real time. As traditional rule-based anomaly detection systems struggle with dynamic, high-volume IoT data, our approach leverages machine learning to provide adaptive, accurate solutions. The system starts by simulating IoT sensor datasets—including both normal and malicious behaviors—followed by preprocessing steps such as normalization and labeling.

Key classifiers, including Isolation Forest and One-Class SVM, are trained to differentiate normal sensor activity from anomalous patterns such as data injection, DoS attacks, and operational irregularities. SmartGuard integrates seamlessly with a Streamlit-powered dashboard, enabling real-time data visualization and anomaly alerts.

The project is highly modular, ensuring scalable, user-friendly deployment across industries such as healthcare, smart homes, and industrial automation. With experimental results showing up to 98% detection accuracy and minimal false positives, SmartGuard offers a significant step forward in IoT security and operational resilience. Future enhancements include model optimization, mobile/edge deployment, and multilingual UI support to broaden accessibility and industrial adoption.

1. Introduction

IoT systems are everywhere—from healthcare to agriculture—but detecting when devices behave abnormally is still a major challenge. Traditional methods can't keep up. SmartGuard brings in machine learning for adaptive, scalable anomaly detection.

2. Literature Review

Existing research highlights the evolution of anomaly detection in IoT—from basic statistical methods to advanced ML models. Key studies include Chandola et al. (2009) on anomaly detection techniques, Diro & Chilamkurti (2018) on distributed detection, Chalapathy & Chawla (2019) on deep learning methods, and Cook et al. (2020) using GANs. These works form the backbone of SmartGuard's ML-driven architecture.

3. Methodology

SmartGuard's pipeline includes data simulation, preprocessing, model training, evaluation, and deployment. The dataset mimics IoT sensor behavior. ML models such as Isolation Forest and One-Class SVM are used. The system is deployed using Streamlit for real-time monitoring.

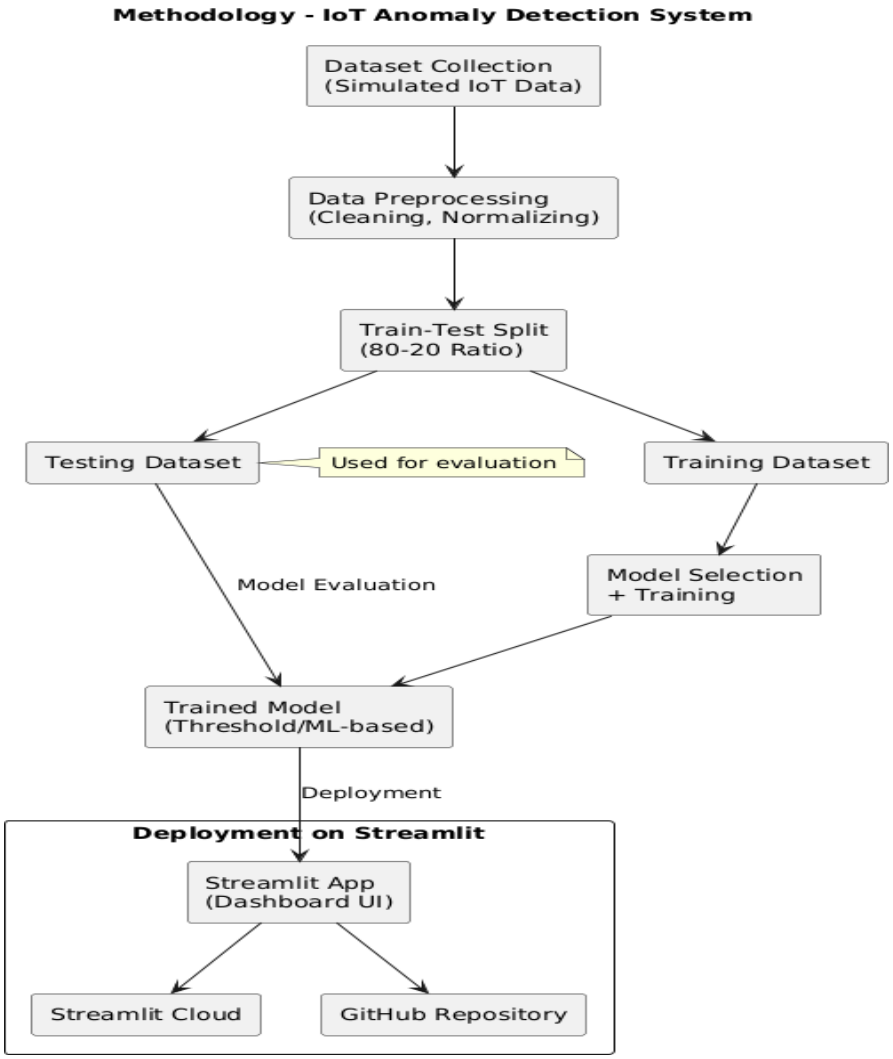
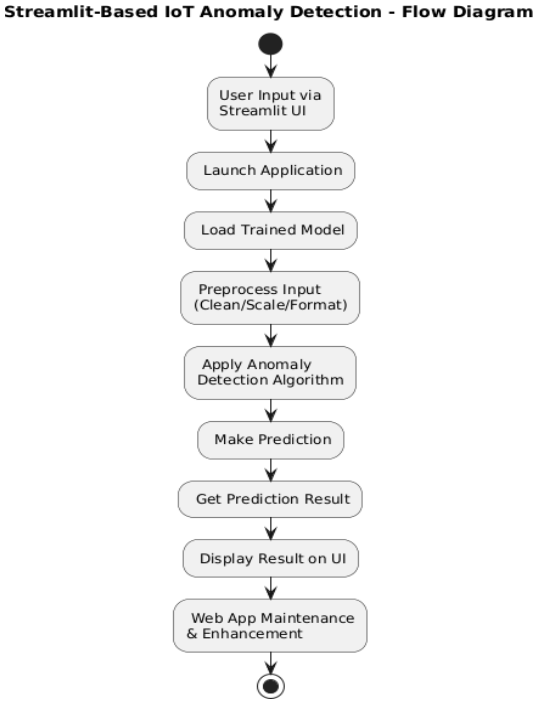


Fig 1: Methodology

3.1 System Architecture

The architecture starts with the Streamlit UI, model loading, data preprocessing, prediction, and output visualization. Real-time sensor data is inputted, classified, and displayed with alerts using a trained ML model.

Fig 2: System Architecture



4. Output Screens

The dashboard displays live input, prediction (normal/anomaly), and sensor trends. Alerts are shown in red with timestamps. Visualization includes charts, gauges, and color-coded indicators.

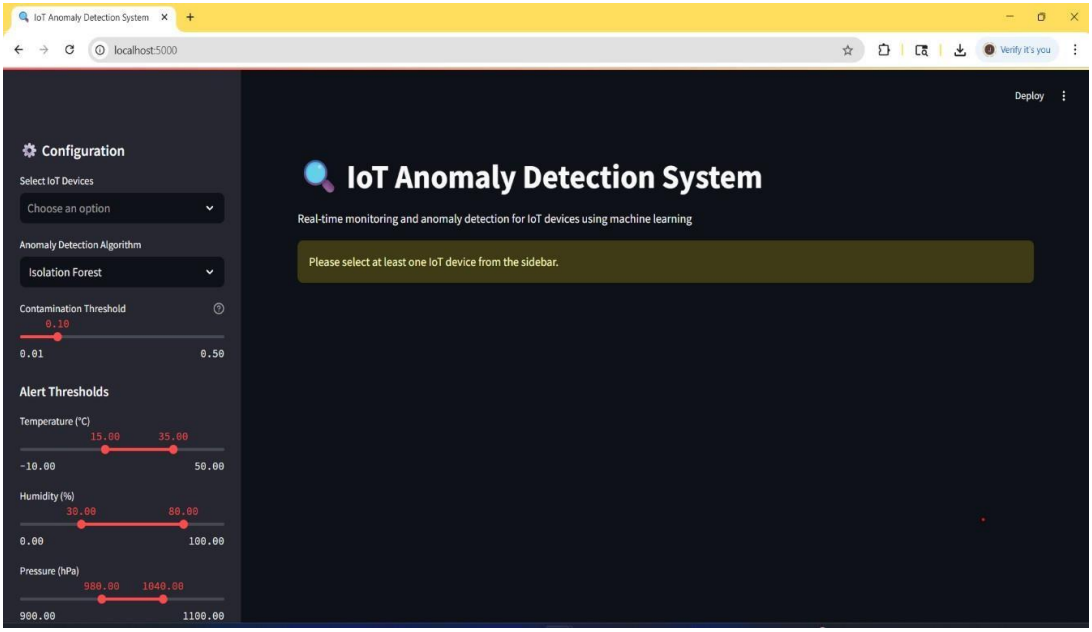


Fig 3: User Interface

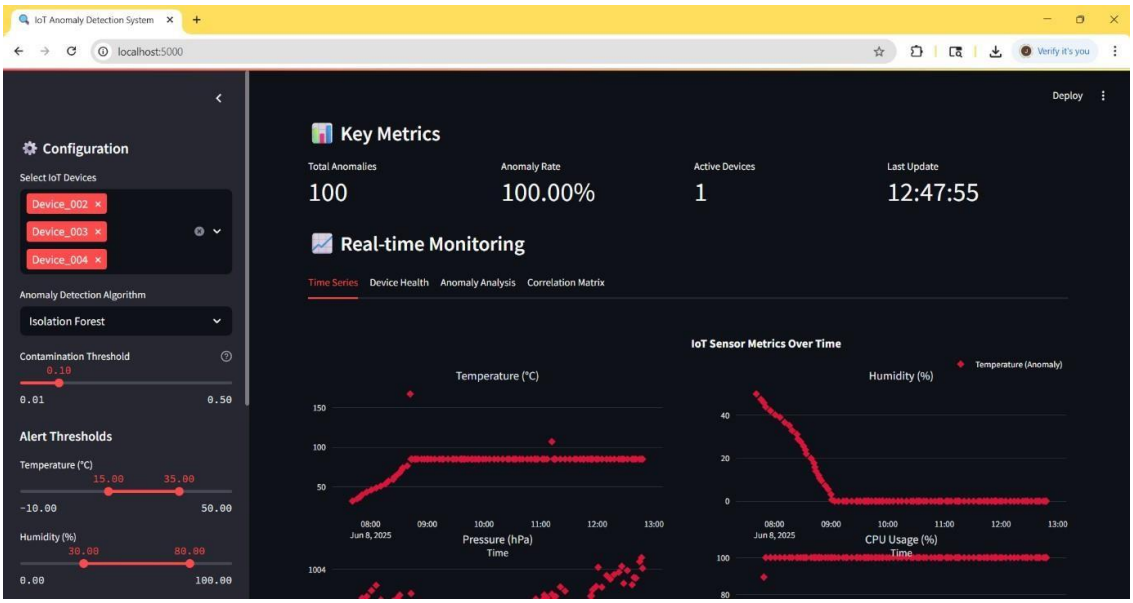


Fig 4: Dashboard

Fig 5: Device Health Overview Details

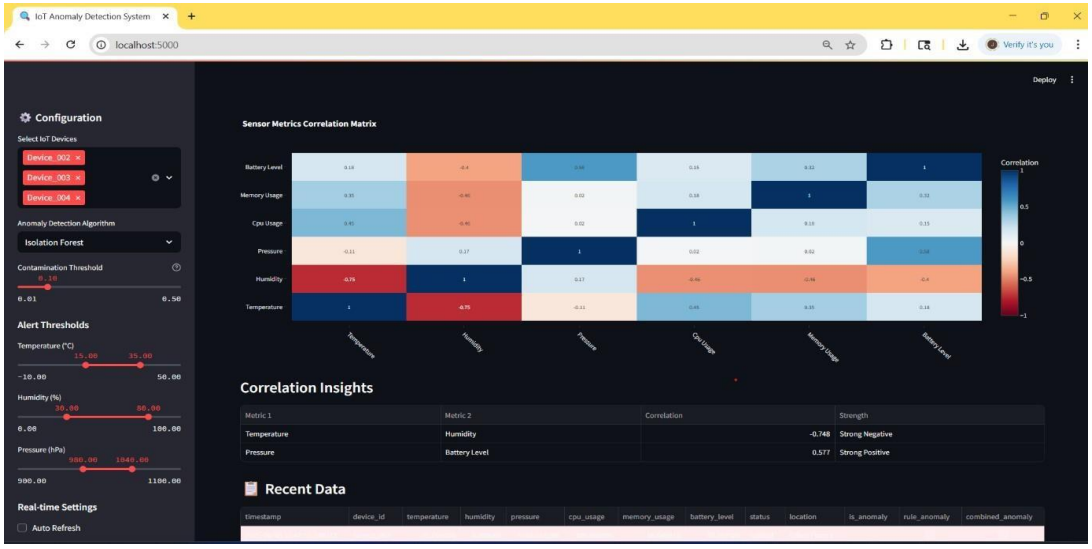


Fig 6: Sensor Correlation Analysis

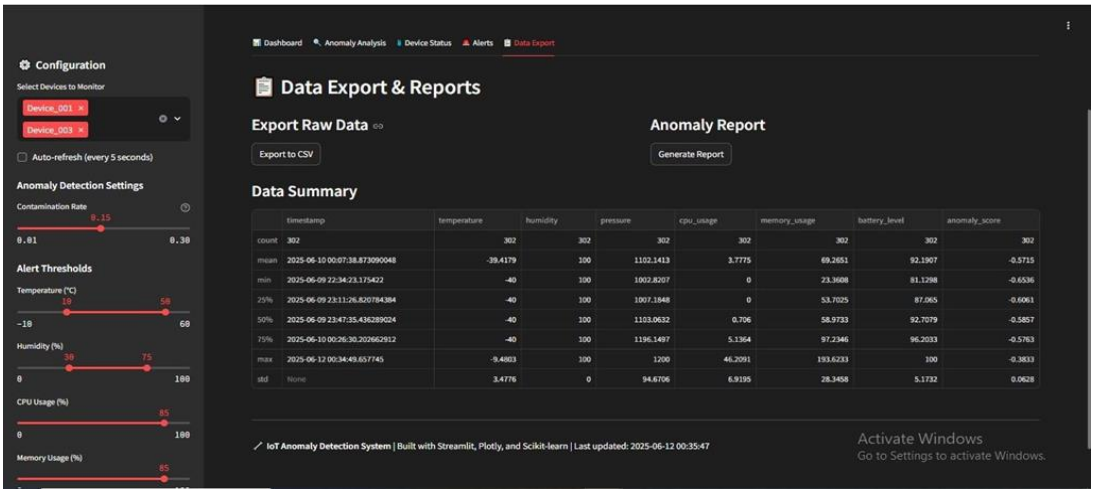


Fig7:Anamoly Data Reports

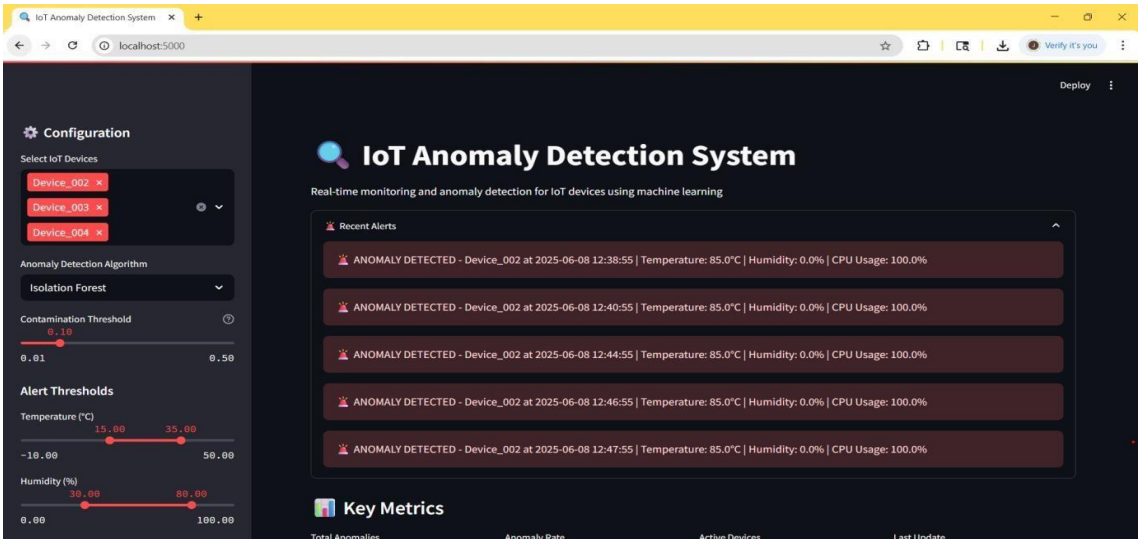


Fig 8: Alert Notification To User

5. Work Flow

The process includes: Dataset simulation → Preprocessing → Model training → Evaluation → Streamlit integration → Real-time input and detection → Alerting and logging → Performance tuning and expansion.

6. Conclusion and Future Scope

SmartGuard effectively detects anomalous behavior in IoT devices using ML. With a scalable design and real-time feedback, it's well-suited for future expansion into mobile, multilingual, and industrial platforms.

Future Scope

Enhancements may include model optimization, edge deployment on IoT gateways, multilingual UIs for broader accessibility, and partnerships with industrial IoT providers for large-scale data validation.

7. Acknowledgement

We express deep gratitude to our mentors, parents, and faculty at ACE Engineering College. Special thanks to Mr. Kalavacherla Kiran for his guidance, and to Dr. P. Chiranjeevi and the CSE-DS team for their support throughout this project.

8. REFERENCES

1. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys.
2. Diro, A. A., & Chilamkurti, N. (2018). Distributed Anomaly Detection in Industrial IoT. Journal of Network and Computer Applications.
3. Chalapathy, R., & Chawla, S. (2019). Deep Learning for Anomaly Detection: A Survey. arXiv:1901.03407.
4. Cook, A. A., Mısırlı, G., & Fan, Z. (2020). Anomaly Detection in IoT Using Generative Adversarial Networks. Sensors, 20(3), 849.
5. Alladi, R., Akhila, A., Hemalatha, K., et al. (2023). Anomaly Detection in IoT Using Machine Learning. ResearchGate.
6. Bayas, I. M., & Joshi, A. S. (2023). Intrusion Detection System for IoT Networks. IJNRD.