



Research Methods and Professional Development

ACFA7004: Assessment Report

Student Name: Gandhi Raj Rakeshkumar

Student ID: 2503898

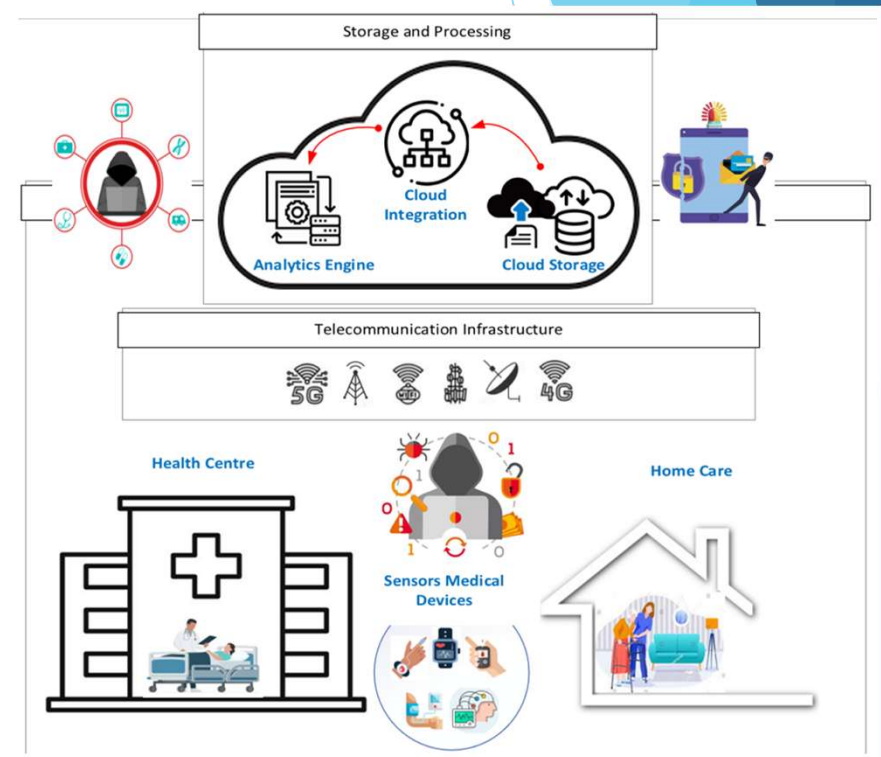
Program: MSC Cybersecurity and Digital Forensics

Submission To: Dr.Suresh Shanmugasunadaram

Topic :- Detection of Unauthorised Access
Attempts in IoT Systems Using Log-Based
Forensics

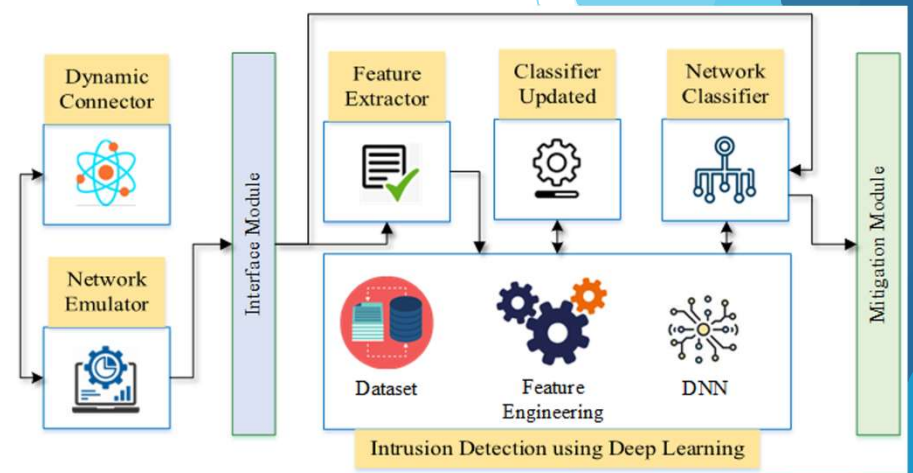
Background & Context

- IoT connects diverse systems across smart homes, healthcare, and industries.
- However, security vulnerabilities arise due to weak authentication and limited resources.
- These issues increase exposure to cyber threats and unauthorised access attempts, requiring advanced detection mechanisms [4], [8].



Problem Statement

- IoT systems generate large volumes of heterogeneous log data, making analysis complex.
- Existing intrusion detection systems lack real-time capabilities and struggle with unknown attacks.
- High false positives reduce reliability, highlighting the need for intelligent, integrated detection solutions [4].



Aim & Objectives

Aim:

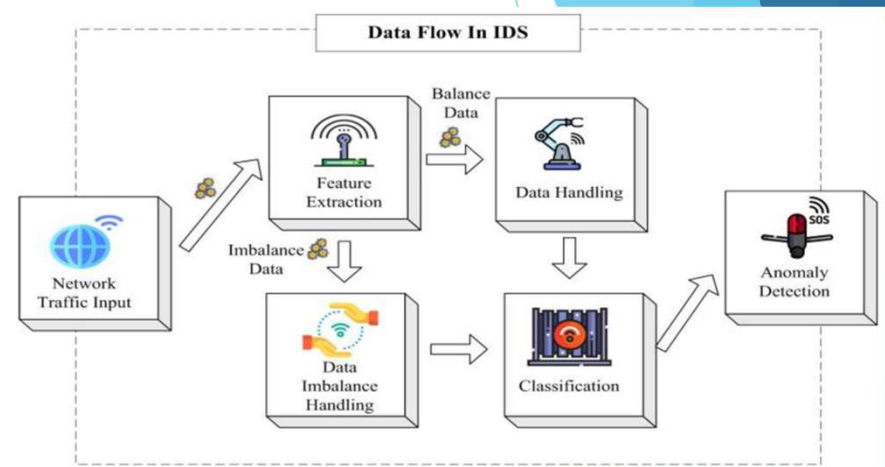
The main goal of the study is to come up with an effective log-based forensic framework to monitor unauthorised attempts of accessing the IoT systems.

Objectives:

- To critically examine the currently used IoT security measures and digital forensic methods so as to understand their advantages and weaknesses.
- To come up with a log-based detection model with the capability to process and analyse the log generated by IoTs effectively.
- To apply anomaly detecting methods to detect suspicious activities by applying machine learning algorithms.
- To measure the performance of the proposed framework in terms of the suitable metrics that include accuracy, precision, recall, and F1-score.
- To make recommendations that will increase the detection capacity in real-time and general efficiency of the system.

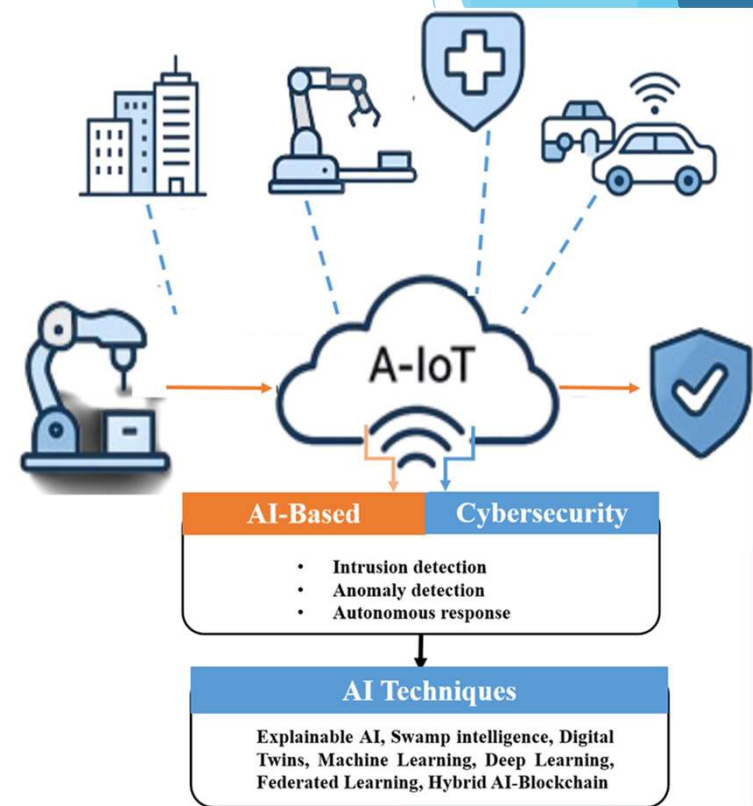
Literature Insights

- Studies highlight IoT vulnerabilities and limitations of traditional IDS.
- Log-based forensics improves investigation capabilities [3].
- Machine learning enhances anomaly detection accuracy [6], [9].
- However, integration between forensic analysis and intelligent detection remains limited [5], [8].



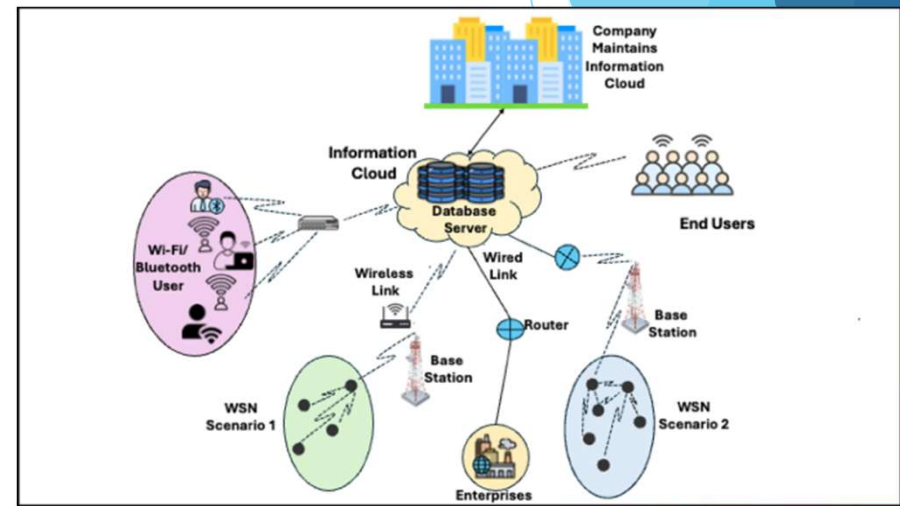
Research Gap

- Current research lacks real-time scalable log analysis frameworks.
- Limited integration of machine learning with forensic log systems exists.
- Challenges remain in handling heterogeneous IoT data and ensuring interpretability of models, indicating a need for unified and intelligent detection frameworks [5], [8].



Methodology

- ┌ This research adopts a Design Science Research approach.
- ┌ A quantitative experimental method is used to develop and evaluate a detection system.
- ┌ The study focuses on building, testing, and refining a machine learning-based framework for IoT intrusion detection.



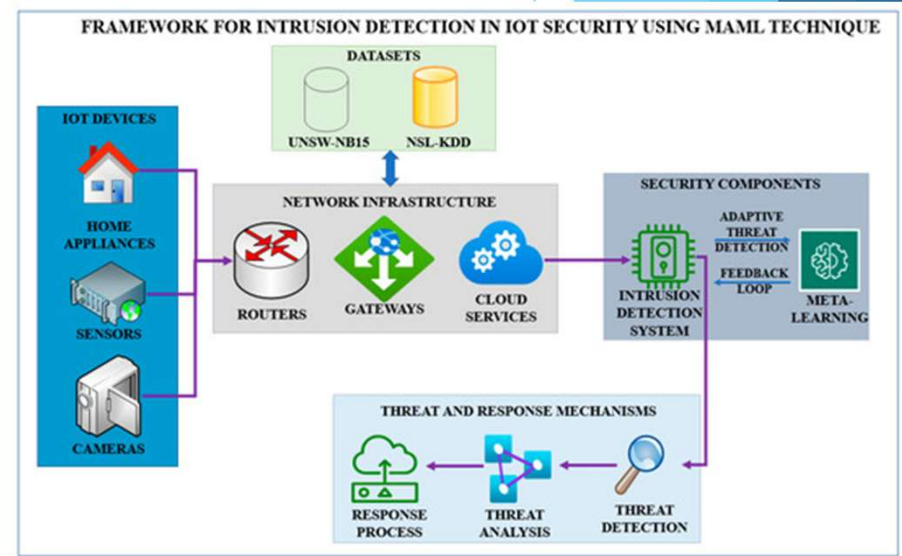
Proposed Framework

- ┌ The framework processes IoT logs through preprocessing, feature extraction, and machine learning-based anomaly detection.
- ┌ It uses datasets such as IoT-23 and TON-IoT.
- ┌ Tools include Python, Scikit-learn, and Wireshark for implementation and analysis [7], [10].



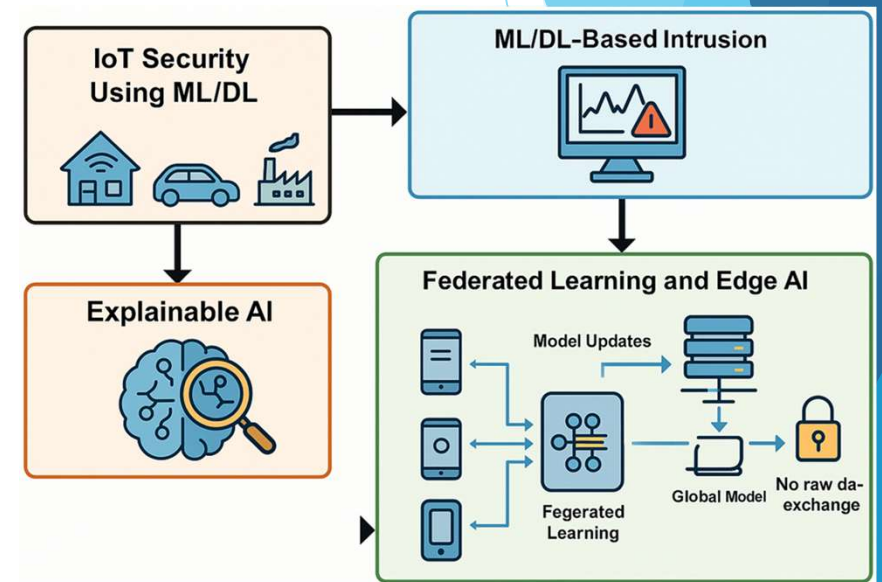
Evaluation & Outcomes

- System performance is evaluated using accuracy, precision, recall, and F1-score.
- Expected outcomes include improved detection accuracy, faster response times, reduced false positives, and a scalable framework suitable for diverse IoT environments [1], [6].



Conclusion & Impact

- IoT security remains a critical challenge.
- This research proposes a unified framework combining log-based forensics and machine learning.
- The solution enhances detection accuracy and supports real-time monitoring, contributing to improved cybersecurity across smart cities, healthcare, and industrial IoT systems [2].



Reference List

- [1] K. S. Adewole, A. Jacobsson, and P. Davidsson, "Intrusion Detection Framework for Internet of Things with Rule Induction for Model Explanation," *Sensors*, vol. 25, no. 6, p. 1845, Mar. 2025, doi: 10.3390/s25061845.
- [2] S. Brotsis et al., "Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems," *Internet of Things*, vol. 24, p. 100968, Oct. 2023, doi: 10.1016/j.iot.2023.100968.
- [3] P. Sharma and L. K. Awasthi, "IoT forensics in ambient intelligence environments: Legal issues, research challenges and future directions," *Journal of Ambient Intelligence and Smart Environments*, vol. 16, no. 1, pp. 73-110, Oct. 2023, doi: 10.3233/ais-220511.
- [4] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, p. 100082, Dec. 2024, doi: 10.1016/j.csa.2024.100082.
- [5] A. J. Aparcana-Tasayco, X. Deng, and J. H. Park, "A systematic review of anomaly detection in IoT security: towards quantum machine learning approach," *EPJ Quantum Technology*, vol. 12, no. 1, Sep. 2025, doi: 10.1140/epjqt/s40507-025-00414-6.
- [6] M. J. C. S. Reis, "AI-Driven anomaly detection for securing IoT devices in 5G-Enabled smart cities," *Electronics*, vol. 14, no. 12, p. 2492, Jun. 2025, doi: 10.3390/electronics14122492.
- [7] S. Anand, L. Kandregula, T. Szydlo, R. Ranjan, and D. N. Jha, "A hybrid monitoring framework for anomaly detection in smart home IoT devices," *ACM Digital Library*, pp. 1-6, Dec. 2025, doi: 10.1145/3773274.3774927.
- [8] Z. A. Haider et al., "A Survey on anomaly detection in IoT: Techniques, challenges, and opportunities with the integration of 6G," *Computer Networks*, vol. 270, p. 111484, Jun. 2025, doi: 10.1016/j.comnet.2025.111484.
- [9] A. M. Almasabi, A. B. Alkhodre, M. Khemakhem, F. Eassa, A. A. A. Sen, and A. Harbaoui, "Internet of Things-Based anomaly detection hybrid framework simulation integration of deep learning and blockchain," *Information*, vol. 16, no. 5, p. 406, May 2025, doi: 10.3390/info16050406.
- [10] H. B. U. Haq et al., "A Deep Dive into Anomaly Detection in IoT Networks, Sensors, and Surveillance Videos in Smart Cities," *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, vol. 87, no. 2, pp. 1-10, Jan. 2026, doi: 10.32604/cmc.2025.073188.

Thank You

