

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 30%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 1 November 2025

Hand-in Date: 25 November 2025

Hand-in Method: Online Submission via E-Learning.

Assignment Report: Literature Review on Anomaly Detection Techniques for Smart IoT Devices

Table of contents:

- Problem Statement
- Research Objectives
- Summary research paper's
- Critical Analysis
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review
- References

Literature Review on Anomaly Detection Techniques for Smart IoT Devices

Problem Statement:

In the rapidly growing ecosystem of smart Internet of Things (IoT) devices, security has become a critical concern. IoT devices are widely deployed in homes, healthcare, transportation, and industrial environments, yet they often operate with limited computational power, memory, and energy resources. These constraints, combined with heterogeneous communication protocols and large-scale connectivity, make IoT networks highly vulnerable to anomalous behaviours such as malicious traffic, device compromise, and data manipulation. If such anomalies are not detected early, they can seriously affect the availability, integrity, and confidentiality of services, which ultimately undermines the reliability and trustworthiness of smart IoT systems.

A variety of anomaly detection solutions have been proposed to address these risks. Deep learning approaches based on autoencoders and deep neural networks have shown high detection rates and low false positives when applied to high-dimensional IoT traffic, particularly on benchmark datasets such as BoT-IoT (Ayad et al., 2025; Sathyabama & Katiravan, 2025). Classical machine learning models and unsupervised methods, including Support Vector Machine (SVM), One-Class SVM (OCSVM), Isolation Forest (IF), and feature-reduction-driven techniques, have also demonstrated competitive performance with potentially lower computational cost (Hamdan et al., 2025; Zahoor et al., 2025). In parallel, recent review and survey works provide taxonomies of deep learning architectures and explore new directions such as quantum machine learning for IoT security (Morshedi & Matinkhah, 2025; Aparcana-Tasayco et al., 2025).

Research Objectives:

- 1. To analyze the current challenges in anomaly detection for smart IoT devices:**
 - To identify key technical and practical limitations reported in recent IoT anomaly detection studies.
 - To examine how resource constraints, data heterogeneity, and evolving attack patterns affect anomaly detection performance and deployment.
- 2. To evaluate existing anomaly detection techniques for IoT networks:**
 - To review and compare statistical, machine learning, deep learning, and hybrid approaches used for IoT anomaly detection.
 - To assess their effectiveness based on datasets, evaluation metrics, and suitability for real-world IoT environments.
- 3. To investigate the impact of model complexity and resource usage:**
 - To analyse the trade-off between detection accuracy and computational cost for different anomaly detection models.
 - To highlight which techniques are more appropriate for constrained edge devices versus cloud-based or fog-based solutions.

4. To identify research gaps and open issues in IoT anomaly detection:

- To synthesize unresolved challenges related to explainability, adversarial robustness, dataset bias, privacy, and scalability.
- To determine where current solutions fall short in supporting large-scale, heterogeneous IoT deployments.

5. To propose directions for future lightweight and adaptable anomaly detection frameworks:

- To outline design principles for developing efficient, scalable, and generalizable anomaly detection solutions tailored to smart IoT ecosystems.
- To provide recommendations that can guide future empirical and implementation-oriented research in IoT security.

Summary of Research Papers:

Paper1: Efficient Real-Time Anomaly Detection in IoT Networks Using One-Class Autoencoder and Deep Neural Network

This paper proposes a lightweight intrusion detection model for IoT networks. The model combines an asymmetric stacked autoencoder with a deep neural network in a one-class learning setting to handle high-dimensional IoT traffic. It is trained only on normal data and then used to detect abnormal behavior in the BoT-IoT dataset. The results show high detection rate and low false positives with short inference time, which makes the approach suitable for real-time IoT security. However, the evaluation is done on benchmark datasets only and does not include large real deployments or very constrained devices.

Paper2: Enhancing Anomaly Detection and Prevention in Internet of Things (IoT) Using Deep Neural Networks and Blockchain Based Cyber Security

This paper introduces an integrated framework that combines deep neural networks (DNNs) with blockchain technology for IoT security. The DNN is used to detect anomalies in network traffic, while blockchain is used to store security events and policies in a tamper-resistant way. The framework aims to provide both accurate detection and strong data integrity and non-repudiation. Experimental results indicate that the DNN achieves good accuracy on IoT attack datasets and that blockchain adds transparency and traceability. The main limitations are higher complexity, extra latency from blockchain operations, and the lack of tests on very large-scale IoT deployments.

Paper3: Feature Reduction and Anomaly Detection in IoT Using Machine Learning Algorithms

This study evaluates several classical machine learning algorithms for IoT anomaly detection on the RT-IoT2022 dataset. The authors test Naïve Bayes, SVM, Decision Tree, XGBoost, Random Forest, and K-Nearest Neighbor. They also apply three feature reduction methods: Principal Component Analysis (PCA), Particle Swarm Optimization (PSO), and Gray Wolf Optimizer (GWO). The results show that most models achieve high performance, and SVM with feature reduction gives the best accuracy (around 99.9%) with good precision and recall. The work is strong in comparing many models and reduction methods, but it is limited to one dataset and does not consider energy or memory cost on real IoT devices.

Paper4: A Comprehensive Review of Deep Learning Techniques for Anomaly Detection in IoT Networks: Methods, Challenges, and Datasets

This review article surveys deep learning approaches for anomaly detection in IoT networks. It summarizes different architectures such as CNNs, LSTMs, autoencoders, GANs, and hybrid models, and discusses how they are applied to traffic data, sensor data, and log data. The paper also reviews commonly used datasets (e.g., CICIDS2017, BoT-IoT, NSL-KDD, TON_IoT) and compares their properties. In addition, it highlights main challenges such as label imbalance, lack of real-world datasets, limited device resources, and difficulties in explainability. The review provides a clear big picture but does not include experimental comparison, so the reader does not see which models are practically best.

Paper5: A Systematic Review of Anomaly Detection in IoT Security: Towards Quantum Machine Learning Approach

This systematic review focuses on anomaly detection for IoT security using machine learning and especially quantum machine learning (QML). The authors analyze existing ML-based anomaly detection methods, feature engineering techniques, and evaluation practices. They then discuss how quantum computing and QML could improve scalability and detection performance compared with classical methods. The paper identifies open issues such as data heterogeneity, real-time processing, privacy in federated learning, and the impact of data drift in 5G/6G IoT environments. The work is mainly conceptual, because there are still few real QML implementations for IoT, so most conclusions are forward-looking.

Paper6: Robust IoT Security Using Isolation Forest and One Class SVM Algorithms

This article presents an anomaly detection framework for IoT networks using two unsupervised algorithms: Isolation Forest (IF) and One-Class Support Vector Machine (OCSVM). Using the TON_IoT dataset, the authors compare IF, OCSVM, and a fusion method called Combined Scoring Anomaly Detection (CSAD). OCSVM achieves the best precision, recall, and accuracy, while remaining lightweight enough for practical deployment. They also use Random Forest feature importance, cross-validation, and adversarial poisoning experiments to test robustness, plus LIME for model interpretability. A limitation is that only one dataset and a limited set of algorithms are considered, and the framework is not tested directly on physical IoT devices.

Critical Analysis:

Across the six papers, there is strong evidence that both traditional machine learning and deep learning can achieve very high accuracy for IoT anomaly detection when good features and datasets are available. Deep models such as autoencoders and DNNs (Papers 1 and 2) handle high-dimensional traffic and can learn complex patterns, while classical models like SVM and OCSVM (Papers 3 and 6) still perform competitively with lower computational cost. Reviews in Papers 4 and 5 show that the research community is actively exploring new deep architectures and even quantum-inspired methods to deal with scalability and complexity.

However, many works still depend on a small number of public datasets and controlled lab settings. Papers 1, 2, 3, and 6 all evaluate on benchmark datasets (BoT-IoT, RT-IoT2022, TON_IoT, etc.) instead of long-term real deployments, so their generalization to heterogeneous IoT environments is uncertain. Resource constraints of edge devices are mentioned but not deeply measured in most papers. In addition, explainability and resilience to adversarial attacks are covered only in a few works (Paper 6 and partly Paper 5), which leaves a gap for practical deployment in sensitive domains.

Connections:

1. All six papers focus on improving **security of IoT networks through anomaly detection**, either with concrete models or survey work.
2. Papers 1, 2, 3, and 6 use **machine learning or deep learning models** directly on IoT traffic or sensor data to detect abnormal behavior.
3. Papers 4 and 5 provide **high-level reviews** that organize existing anomaly detection approaches and highlight open research challenges.
4. Several works share **common datasets** such as BoT-IoT and TON_IoT and use standard metrics (accuracy, precision, recall, F1-score), which allows basic comparison across studies.
5. Papers 2 and 5 both look at **advanced architectures and technologies** (blockchain and quantum computing) to improve trust, privacy, or scalability in IoT security.
6. Papers 3 and 6 both emphasize **lightweight or efficient solutions** using feature reduction or unsupervised models to fit resource-constrained environments.

Conflicts between the findings:

1. Deep learning papers (1 and 2) suggest that complex neural networks are needed for high accuracy, while Papers 3 and 6 show that **classical or unsupervised models** (SVM, OCSVM, IF) can achieve similar or even better performance with lower cost.
2. Some works assume that **centralized training in the cloud** is acceptable (Papers 1, 2, 3), but the reviews (Papers 4 and 5) stress that centralized approaches can create privacy risks and scalability issues, and propose federated or quantum-enabled solutions instead.
3. Paper 2 argues that **blockchain integration** is a practical way to enhance security, while Paper 6 focuses on keeping the system lightweight and does not include heavy components like blockchain; this shows a tension between **strong integrity guarantees** and **minimal resource usage**.
4. Reported accuracies are often extremely high (around 99–100% in Papers 1 and 3), but Paper 4 notes that such results may be optimistic because of **dataset bias, limited attack diversity, or simple train/test splits**, so the real performance in complex environments may be lower.

Synthesis Matrix for Literature Review:

Study	Authors	Year	Research design / data	Methodology	Key findings / results	Main limitations
Paper1	Ayad, El-Gayar, Hikal, & Sakr	2025	Experimental; BoT-IoT dataset for IoT network traffic	Asymmetric stacked autoencoder + DNN with one-class learning	High detection rate and low false positives; suitable for real-time IDS in IoT networks (MDPI)	Tested only on benchmark data; no hardware or energy evaluation on real devices
Paper2	Sathyabama & Katiravan	2025	Experimental; IoT traffic datasets with attacks	Deep neural network for anomaly detection + blockchain layer for secure logging and prevention	Integrated DNN-Blockchain framework improves detection and provides tamper-proof security records (Nature)	Higher complexity and latency; scalability of blockchain in very large IoT not fully studied
Paper3	Hamdan, Tahboush, Adawy, Alwada'n, & Ghwanmeh	2025	Experimental; RT-IoT2022 dataset	Several ML models (NB, SVM, DT, XGBoost, RF, K-NN)	SVM with feature reduction achieves $\approx 99.9\%$ accuracy; feature reduction improves	Only one dataset; no analysis of model deployment cost on

				+ feature reduction (PCA, PSO, GWO)	performance and reduces dimensions (thesai.org)	constrained IoT nodes
Paper4	Morshedi & Matinkhah	2025	Review of many experimental studies and datasets	Structured literature review of DL architectures (CNN, LSTM, AE, GAN, hybrids) for IoT anomaly detection	Provides taxonomy of methods and datasets; identifies challenges like imbalance, data quality, and resource limits (Directory of Open Access Journals)	No direct experiments; limited guidance on which models are best for specific IoT scenarios
Paper5	Aparcana-Tasayco, Deng, & Park	2025	Systematic review with defined protocol	Reviews ML-based anomaly detection and explores quantum machine learning directions	Shows potential of QML to overcome computational limits and improve detection; summarizes future research needs (SpringerOpen)	Few concrete QML implementations; conclusions mainly conceptual and based on early works
Paper6	Zahoor, Abbasi, Babar, & Aljohani	2025	Experimental; TON_IoT dataset	Unsupervised anomaly detection using Isolation Forest, OCSVM, and fusion CSAD + feature importance and LIME	OCSVM gives best precision, recall, and accuracy; demonstrates that lightweight unsupervised models can protect IoT networks (Nature)	Only compares three algorithms; experiments limited to one dataset and simulated environment

References:

- Ayad, A. G., El-Gayar, M. M., Hikal, N. A., & Sakr, N. A. (2025). Efficient real-time anomaly detection in IoT networks using one-class autoencoder and deep neural network. *Electronics*, 14(1), 104. <https://doi.org/10.3390/electronics14010104>
- Hamdan, A., Tahboush, M., Adawy, M., Alwada'n, T., & Ghwanmeh, S. (2025). Feature reduction and anomaly detection in IoT using machine learning algorithms. *International Journal of Advanced Computer Science and Applications*, 16(1), 463–470. <https://doi.org/10.14569/IJACSA.2025.0160146>
- Morshedi, R., & Matinkhah, S. M. (2025). A comprehensive review of deep learning techniques for anomaly detection in IoT networks: Methods, challenges, and datasets. *Engineering Reports*, 7(9), e70415. <https://doi.org/10.1002/eng2.70415>
- Sathyabama, A. R., & Katiravan, J. (2025). Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security. *Scientific Reports*, 15, 22369. <https://doi.org/10.1038/s41598-025-04164-4>
- Zahoor, A., Abbasi, W., Babar, M. Z., & Aljohani, A. (2025). Robust IoT security using isolation forest and one class SVM algorithms. *Scientific Reports*, 15, 36586. <https://doi.org/10.1038/s41598-025-20445-4>
- Aparcana-Tasayco, A. J., Deng, X., & Park, J. H. (2025). A systematic review of anomaly detection in IoT security: Towards quantum machine learning approach. *EPJ Quantum Technology*, 12, 112. <https://doi.org/10.1140/epjqt/s40507-025-00414-6>