

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 50%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 15 November 2025

Hand-in Date: 20 December 2025

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

Research Proposal (Final Research Project)

Literature Review on Anomaly Detection Techniques for Smart IoT Devices

Table of Contents

Abstract	2
Introduction.....	3
Background	3
Problem statement	3
Research objective.....	4
Research scope	5
Literature review	6
Summary of Research Papers:	6
Critical Analysis:	9
Connections:.....	10
Conflicts Between the Findings:	11
Synthesis Matrix for Literature Review:	12
Research methodology.....	14
Search strategy and sources	14
Inclusion and exclusion criteria	14
Studies are included if they:.....	14
Studies are excluded if they:	14
Selection and synthesis process	15
Expected outcomes	15
This research proposal is expected to produce:.....	15
Gantt chart	15
References	17

Abstract

The rapid proliferation of smart Internet of Things (IoT) devices across domains such as smart homes, healthcare, transportation, and industrial systems has introduced significant security challenges. IoT environments are characterized by heterogeneous traffic, large-scale connectivity, and continuous data streams, while most devices operate under strict constraints in computational power, memory, energy, and bandwidth. These characteristics make IoT networks highly vulnerable to anomalous behaviours, including malicious traffic, device compromise, and data manipulation.

Anomaly detection has therefore become a critical mechanism for enhancing IoT security, and a wide range of techniques has been proposed in recent years, including traditional machine learning, deep learning, unsupervised approaches, and hybrid frameworks. Despite promising results reported in controlled experimental settings, practical deployment remains challenging due to dataset dependency, limited real-device validation, computational overhead, lack of interpretability, privacy constraints, and degradation under non-stationary traffic conditions such as concept drift.

This research proposal reviews and synthesizes recent studies on anomaly detection techniques for smart IoT environments, critically analyzes methodological trends and deployment trade-offs, and outlines a brief methodology and project plan to guide future work. The expected outcome is a clearer pathway toward lightweight, robust, explainable, and trustworthy anomaly detection solutions suitable for real-world IoT deployments.

Introduction

Smart IoT systems are increasingly deployed in critical and everyday settings, enabling continuous sensing, automation, and connectivity. However, the same connectivity that enables IoT functionality also expands the attack surface, creating opportunities for malicious behaviours such as intrusion attempts, botnet activity, data exfiltration, and service disruption. Anomaly detection is widely used as a key security capability because it can identify abnormal patterns that may not match known signatures, supporting early warning and faster incident response. This project focuses on reviewing, analyzing, and planning research around anomaly detection techniques that can operate effectively within the constraints and dynamics of IoT networks.

Background

IoT networks are composed of diverse devices and protocols, producing large volumes of traffic with varying behavioural patterns depending on device type, application context, and environmental conditions. These networks often operate under strict resource constraints at the edge, while facing evolving attack strategies and shifting data distributions over time. As a result, security monitoring in IoT requires methods that are accurate, efficient, scalable, and robust to changes in traffic behaviour. Recent literature proposes many approaches—ranging from classical machine learning and one-class learning to deep learning, explainable intrusion detection, blockchain-supported security logging, federated learning, and drift-aware detection—yet real-world feasibility and trustworthiness remain central concerns.

Problem statement

Smart Internet of Things (IoT) environments are expanding rapidly across domains such as smart homes, healthcare, transportation, and industrial systems. However, IoT devices typically operate under strict constraints in memory, processing power, energy, and bandwidth, while generating large, heterogeneous, and continuously evolving network traffic. These characteristics make IoT ecosystems highly vulnerable to anomalous behaviours, including malicious traffic, device compromise, and data manipulation. If anomalies are not detected early and reliably, they can undermine the availability, integrity, and confidentiality of services and reduce trust in IoT deployments.

Although many anomaly and intrusion detection approaches have been proposed—ranging from traditional machine learning to deep learning and hybrid methods—practical deployment remains challenging. Current solutions often show strong performance in controlled experiments but may fail to generalize across diverse IoT settings due to dataset dependency, limited real-device evaluation, high computational cost, lack of interpretability, privacy concerns in centralized learning, and performance degradation under non-stationary data streams (e.g., concept drift). As a result, there is still a need for anomaly detection solutions that balance detection effectiveness with real-world feasibility in resource-constrained and dynamic IoT networks.

Therefore, the core problem addressed in this work is: How can anomaly detection techniques for smart IoT networks be designed and evaluated to achieve high detection performance while remaining lightweight for constrained devices, robust to evolving and non-stationary traffic, and suitable for trustworthy deployment in real-world IoT environments?

Research objective

1. To identify and synthesize the key challenges that limit effective anomaly detection in smart IoT environments, with particular focus on resource constraints, heterogeneous traffic, and evolving attack behaviours.
2. To review and compare major anomaly and intrusion detection approaches used in IoT security (traditional machine learning, deep learning, and hybrid methods) based on commonly reported evaluation metrics and experimental practices.
3. To evaluate the practicality of existing approaches by examining trade-offs between detection performance and deployment feasibility, including computational cost, model size, latency, scalability, and suitability for edge versus cloud settings.
4. To identify research gaps and propose directions for developing more trustworthy IoT anomaly detection solutions, emphasizing explainability, robustness to non-stationary data (concept drift), and privacy-preserving learning in distributed IoT networks.

Research scope

This research proposal focuses on anomaly and intrusion detection techniques designed for smart IoT environments, with emphasis on approaches reported between 2024 and 2025 in peer-reviewed literature. The scope includes classical machine learning, deep learning, unsupervised and one-

class detection, explainable intrusion detection, federated learning for privacy-aware detection, blockchain-supported security event integrity, and drift-aware detection for non-stationary IoT data streams. The scope is limited to literature-based synthesis and planning; it does not include implementing or experimentally benchmarking new models within this report. Additionally, conclusions are constrained by differences in datasets, evaluation settings, and the limited availability of long-term real-device deployment studies in the reviewed literature.

Literature review

Summary of Research Papers:

Paper 1 (Ayad et al., 2025) — One-Class Autoencoder + DNN for Real-Time IoT Anomaly Detection

This study proposes a lightweight intrusion detection approach that combines an asymmetric stacked autoencoder with a deep neural network under a one-class learning setting. The model is trained using only normal traffic and then applied to detect abnormal behaviour in the BoT-IoT dataset. Reported outcomes indicate a high detection rate with low false positives and short inference time, supporting suitability for real-time IoT security monitoring. A key limitation is that evaluation is limited to benchmark datasets and does not fully validate performance on highly constrained devices or large real deployments.

Paper 2 (Sathyabama & Katiravan, 2025) — DNN + Blockchain for Detection and Tamper-Proof Security Records

This paper presents a framework that integrates deep neural networks (DNNs) for anomaly detection with blockchain to store security events and policies in a tamper-resistant manner. The DNN component detects anomalies in IoT traffic, while blockchain supports integrity, transparency, and traceability of security records. Experimental discussion suggests good detection effectiveness and added trust guarantees through immutable logging. The main drawbacks are increased system complexity and latency due to blockchain operations, with limited evidence of scalability in very large IoT environments.

Paper 3 (Hamdan et al., 2025) — Classical ML + Feature Reduction on RT-IoT2022

This work evaluates multiple machine learning models (e.g., Naïve Bayes, SVM, Decision Tree, XGBoost, Random Forest, K-NN) for anomaly detection using the RT-IoT2022 dataset. The authors also apply feature reduction techniques including PCA, PSO, and GWO to reduce dimensionality and improve efficiency. The results reported in the review indicate very high performance overall, with SVM plus feature reduction achieving around 99.9% accuracy alongside strong precision and recall. Limitations include reliance on a single dataset and the lack of direct measurement of deployment costs (energy/memory) on real IoT devices.

Paper 4 (Morshedi & Matinkhah, 2025) — Review of Deep Learning Methods, Challenges, and Datasets

This paper is a structured review of deep learning techniques used for anomaly detection in IoT networks, covering architectures such as CNNs, LSTMs, autoencoders, GANs, and hybrid models. It also summarizes commonly used datasets (e.g., CICIDS2017, BoT-IoT, NSL-KDD, TON_IoT) and highlights recurring research challenges such as label imbalance, limited real-world datasets, constrained device resources, and explainability. Its key contribution is organizing the field through taxonomy and problem framing rather than proposing a new algorithm. However, the paper does not provide direct experimental comparisons that would clearly identify which models perform best under specific IoT deployment conditions.

Paper 5 (Aparcana-Tasayco et al., 2025) — Systematic Review Toward Quantum Machine Learning for IoT Security

This systematic review examines anomaly detection for IoT security with emphasis on machine learning practices and the emerging direction of quantum machine learning (QML). It analyses existing ML-based detection methods and then argues that QML may help address computational constraints and scalability barriers faced by classical approaches. The review also surfaces open issues such as heterogeneity, real-time constraints, privacy (including federated settings), and the growing impact of data drift in advanced IoT networks. A major limitation is that the discussion remains largely conceptual because there are still few concrete QML implementations validated in realistic IoT scenarios.

Paper 6 (Zahoor et al., 2025) — Unsupervised IF/OCSVM + Fusion (CSAD) on TON_IoT with Robustness + Explainability

This paper proposes an unsupervised anomaly detection framework for IoT networks using Isolation Forest (IF), One-Class SVM (OCSVM), and a fusion approach called Combined Scoring Anomaly Detection (CSAD) evaluated on the TON_IoT dataset. The study reports that OCSVM achieves the best precision, recall, and accuracy among the compared approaches while remaining lightweight enough to be practical. The authors additionally use feature importance, cross-validation, adversarial poisoning experiments to test robustness, and LIME to support interpretability. Limitations include evaluation on a single dataset, a restricted set of algorithms, and the lack of direct testing on physical IoT hardware.

Paper 7 (Sharma et al., 2024) — Explainable Deep Learning IDS for IoT (XAI Focus)

This study targets intrusion detection for IoT networks using deep learning while emphasizing explainability to support trust and operational decision-making. It discusses implementing deep learning-based IDS and highlights the use of explainability methods (e.g., SHAP/LIME-style explanations) to make predictions more transparent. The paper also points to practical concerns

such as class imbalance and how imbalance can distort reported performance in intrusion detection settings. A key limitation is that explainability does not automatically guarantee generalization, and performance can still depend strongly on dataset characteristics and attack diversity.

Paper 8 (Albanbay et al., 2025) — Federated Learning IDS: Performance Evaluation and Data Scaling

This paper evaluates federated learning (FL) for intrusion detection in IoT environments, focusing on how scaling and distribution of client data affect model quality and training stability. The authors emphasize that many real FL scenarios involve non-iid (non-identically distributed) data, which can create performance drops and fairness issues across clients. The reported results show strong overall performance under the studied setup, with accuracy and precision typically around ~98% and recall around ~95% in the stated experiments. The main limitation is that FL performance is sensitive to client data imbalance and communications overhead assumptions, which can differ significantly across real IoT deployments.

Paper 9 (Chu et al., 2024) — Concept Drift Localization for IoT Data Streams (EMNCD)

This work addresses intrusion detection in streaming IoT data where the underlying distribution changes over time (concept drift). The authors propose an ensemble non-parametric drift detection method (EMNCD) and frame drift localization as a practical requirement for reliable detection in non-stationary environments. In experiments, EMNCD is reported to achieve high detection quality and low false positives, with results including approximately 97.81% accuracy, 96.89% F1-score, 96.39% precision, 97.47% recall, and 0.88% false positives in the provided evaluation. A core limitation is that stream environments can be highly sensitive to scenario design, and mapping drift metrics to realistic IoT attack conditions can be challenging.

Paper 10 (Misrak & Melaku, 2025) — Lightweight IDS with Feature Engineering + Dynamic Quantization

This paper proposes a lightweight IDS approach that combines deep learning with improved feature engineering and advanced dynamic quantization to reduce model size while retaining strong accuracy. The method uses a hybrid DNN–BiLSTM architecture with a two-stage feature selection strategy and quantization to compress the model footprint. Reported results show high accuracy (around 99.73%) with a compact model size (~25.6 KB) on CIC-IDS2017, and similarly high accuracy (around 93.95%) with ~31.3 KB on CIC-IoT2023. The main limitation is that deployment realism (hardware, latency, and energy constraints) and cross-dataset generalization remain critical concerns for practical adoption in heterogeneous IoT settings.

Critical Analysis:

Across the selected literature, anomaly detection for IoT security shows consistently strong performance in controlled evaluations, but several practical deployment gaps remain. A repeated limitation is heavy reliance on benchmark datasets rather than long-term, heterogeneous real deployments. For example, the one-class autoencoder + DNN approach reports strong real-time suitability but is still evaluated mainly on public benchmark traffic datasets, leaving uncertainty about robustness under diverse device types, noisy sensing conditions, and evolving attacker behavior. Likewise, blockchain-integrated detection frameworks improve auditability and integrity, yet they introduce extra system complexity and latency, and often lack validation at large IoT scale.

A second major challenge is the resource constraint reality of IoT/edge nodes (CPU, memory, energy). While feature reduction and lightweight modeling can push accuracy very high, studies still commonly omit energy and memory cost measurements on real devices, making it difficult to judge deployability on constrained hardware. This limitation also appears in unsupervised solutions (e.g., Isolation Forest / One-Class SVM), where the scope is often restricted to a single dataset and a narrow algorithm set, with limited direct physical device testing. Federated learning work helps address privacy and decentralization needs, but it introduces communication overhead, convergence challenges under non-IID data, and risks that rare attack patterns become underrepresented when local datasets are small or imbalanced. In addition, federated settings raise security concerns such as model-poisoning attacks, where malicious clients can manipulate updates and degrade the global model if robust aggregation is not used.

Finally, multiple papers highlight gaps related to non-stationarity and trust. IoT traffic is frequently streaming and evolving, which makes concept drift a central issue; drift-detection methods can be sensitive to noise/outliers and may produce false drift reports, motivating ensemble and adaptive strategies. Explainability is increasingly treated as necessary for operational trust (e.g., using SHAP/LIME), yet real datasets can be class-imbalanced, meaning high overall accuracy may hide weak performance on minority attack classes. Overall, the evidence supports high detection capability in research settings, but the field still needs stronger validation under realistic IoT constraints (resource profiling on devices, cross-dataset generalization, drift-aware evaluation, and adversarially robust learning) to close the gap between lab performance and real-world adoption.

Connections:

Several clear connections emerge across the ten studies, showing strong agreement on the main drivers, solution directions, and evaluation patterns for anomaly/intrusion detection in smart IoT environments:

1. IoT security is constrained by resources and heterogeneity
2. Most papers recognize that IoT devices operate with limited memory, compute, and energy, while producing heterogeneous traffic. This shared assumption directly motivates lightweight detection, feature reduction, and efficient learning strategies.
3. High detection performance is commonly reported, but mostly on benchmark datasets

Experimental papers frequently demonstrate strong accuracy/precision/recall using public IDS/IoT datasets (e.g., BoT-IoT, TON_IoT, RT-IoT2022, CIC-IDS2017, CIC-IoT2023). This shows a shared evaluation trend: strong lab performance, often under controlled conditions.

4. Two dominant technical directions: deep learning vs. classical/unsupervised ML

The literature consistently clusters into:

- a. Deep learning approaches (e.g., autoencoders, DNN, BiLSTM) aiming for high detection capacity on complex patterns.
- b. Classical ML / unsupervised methods (e.g., SVM/OCSVM, Isolation Forest) often emphasized as simpler and potentially lighter for constrained IoT settings.

Several papers implicitly support combining these directions through hybrid pipelines (feature engineering + compressed deep models).

5. Efficiency improvements are repeatedly pursued through feature engineering and compression

Papers using feature reduction (e.g., PCA/optimization) and lightweight modeling align strongly with the trend of making IDS deployable on edge devices. Misrak & Melaku (2025) connects to this directly via quantization and compact model size.

6. Trust and operational usability are emerging as cross-cutting priorities

Multiple studies emphasize that raw detection accuracy is not enough for real-world adoption. Two major shared “trust” themes appear:

- a. Explainability (XAI) to make decisions understandable (e.g., Sharma et al., 2024; Zahoor et al., 2025).
- b. Integrity and governance of security records (e.g., blockchain-based logging in Sathyabama & Katiravan, 2025).

7. The field is increasingly acknowledging dynamic environments and changing data

Concept drift (Chu et al., 2024) and discussions in review papers align with a broad recognition that IoT traffic evolves over time, and models must remain reliable under non-stationary conditions.

8. Reviews and surveys reinforce the same gaps identified by experimental work

The review-based papers (Morshedi & Matinkhah, 2025; Aparcana-Tasayco et al., 2025) connect tightly with the experimental findings by repeatedly pointing to the same issues: dataset realism, resource constraints, scalability, and the need for more robust/transparent solutions.

Conflicts Between the Findings:

Although the reviewed studies share the goal of improving IoT anomaly and intrusion detection, they differ in several important ways, and these differences lead to conflicting conclusions about what “works best” in practice.

1. Deep learning vs. classical/unsupervised methods (accuracy vs. feasibility)

2. Deep learning approaches (e.g., autoencoder–DNN and DNN–BiLSTM) often report very high detection performance on benchmark datasets, suggesting strong capability for complex IoT attack patterns. However, classical and unsupervised approaches (e.g., OCSVM and Isolation Forest) are frequently presented as more feasible for deployment due to simpler computation and lower operational requirements. As a result, the literature does not agree on a single “best” method; instead, results depend on whether the main objective is maximum accuracy or practical deployability.

3. Feature reduction and model compression: performance gain vs. information loss risk

Studies using feature reduction and optimization techniques report improved efficiency and, in some cases, improved accuracy. In contrast, other work suggests that aggressive reduction or compression can remove informative signals and may reduce generalization when traffic patterns change. This creates a trade-off: feature reduction may improve speed and resource usage, but it can also increase the risk of missing subtle anomalies in diverse IoT settings.

4. Centralized learning vs. federated learning (performance stability vs. privacy and distribution)

Centralized training typically assumes full access to data, which can yield stable performance in controlled experiments. Federated learning, on the other hand, supports privacy and decentralization but introduces challenges such as non-IID client data, communication overhead, and uneven performance across clients. Consequently, some findings emphasize that federated IDS can reach strong performance, while others highlight that federated performance may drop under realistic client heterogeneity and data imbalance.

5. Explainability: improved trust vs. added complexity and limited practical validation

Explainable IDS approaches argue that interpretability is essential for trust and operational decision-making. However, explainability methods may add computational overhead and are not consistently validated under real-time, resource-limited conditions. Therefore, the literature disagrees on whether explainability can be treated as a standard requirement in lightweight IoT IDS deployments or whether it remains a secondary feature.

6. Static evaluation vs. streaming environments with concept drift

Many studies evaluate detection on static datasets and report high accuracy, implicitly assuming stable data distributions. In contrast, drift-focused research shows that IoT data streams can shift over time, which may degrade model performance if drift is not detected and handled. This creates a conflict in evaluation assumptions: static benchmark success does not necessarily imply long-term reliability in non-stationary IoT networks.

Overall, these conflicts indicate that IoT anomaly detection performance is highly dependent on dataset choice, evaluation setting, and deployment constraints. The most suitable approach is therefore context-dependent rather than universal.

Synthesis Matrix for Literature Review:

Paper	Study Authors (Year)	Research design / data	Methodology	Key findings / results	Main limitations
1	Ayad, El-Gayar, Hikal, & Sakr (2025)	Experimental; BoT-IoT dataset (IoT network traffic)	Asymmetric stacked autoencoder + DNN with one-class learning	High detection rate and low false positives; short inference time → suitable for real-time IDS in IoT networks	Tested mainly on benchmark data; no evaluation on real constrained devices (hardware/energy)
2	Sathyabama & Katiravan (2025)	Experimental; IoT traffic datasets with attacks	DNN anomaly detection + blockchain layer for secure logging/prevention	Improves anomaly detection + provides tamper-proof security records (traceability/integrity)	Higher complexity/latency; blockchain scalability in large IoT not fully tested
3	Hamdan et al. (2025)	Experimental; RT-IoT2022 dataset	ML models (NB, SVM, DT, XGBoost, RF, K-NN) + feature reduction (PCA/PSO/GWO)	SVM with feature reduction achieves ~99.9% accuracy; reduction improves performance & dimensionality	One dataset; no deployment-cost analysis for constrained IoT nodes
4	Morshedi & Matinkhah (2025)	Review of many studies/datasets	Review of DL architectures (CNN/LSTM/AE/GAN/hybrids) for IoT anomaly detection	Taxonomy of methods & datasets; highlights issues (imbalance, data quality, resource limits)	No direct experiments; limited guidance on best model per scenario
5	Aparcana-Tasayco, Deng, & Park (2025)	Systematic review with defined protocol	Reviews ML-based anomaly detection + explores quantum ML directions	Summarizes future research needs; positions QML as potential path for computational limits	Few concrete QML implementations; mostly conceptual/early evidence
6	Zahoor, Abbasi, Babar, &	Experimental; TON IoT dataset	Unsupervised IF + OCSVM + fusion CSAD; feature importance + LIME	OCSVM shows best precision/recall/accuracy;	Only 3 algorithms; single dataset;

	Aljohani (2025)			lightweight unsupervised protection is feasible	simulated environment (no real device testing)
7	Sharma, Sharma, Lal, & Roy (2024)	Experimental; NSL-KDD + UNSW-NB15	DNN and CNN IDS + filter-based feature selection; explainability via LIME & SHAP	DL models achieve higher accuracy on both datasets; fewer features improve speed/accuracy; explanations increase trust	Dataset not balanced → majority-class bias in accuracy
8	Albanbay et al. (2025)	Federated learning empirical study; CICIOT2023; simulates up to ~150 IoT devices + Raspberry Pi 5 deployment tests	FL training of DNN vs CNN vs CNN+BiLSTM; evaluates accuracy, convergence speed, and inference costs (latency/model size)	CNN best trade-off: ~98% accuracy with low latency/compact footprint; CNN+BiLSTM slightly higher (~99%) but higher compute cost; feasible on edge hardware	More complex models raise computational cost significantly (latency/footprint considerations)
9	Chu et al. (2024)	IoT data streams / non-stationary setting; edge-IIoTset intrusion dataset + synthetic tests	Concept drift localization via EMNCD (ensemble non-parametric tests) + online iForest outlier detection + drift adaptation WOA-XGBoost	EMNCD improves drift point localization and reliability; drift-aware WOA-XGBoost improves accuracy/F1/precision/recall vs no drift handling	Performance depends on detection window & step size selection in practice
10	Misrak & Melaku (2025)	Experimental; CIC-IDS2017 and CIC-IoT2023	Hybrid DNN-BiLSTM + improved feature engineering (RAL-MIFS + two-stage IPCA) + QAT/PTDQ quantization + Optuna tuning	Competitive accuracy with lightweight footprint: 99.73% (CIC-IDS2017) and 93.95% (CIC-IoT2023); model size ~25.6 KB / 31.3 KB	Real deployment still needs careful balancing of accuracy/latency/resource efficiency and scalability across diverse IoT platforms

Research methodology

This research proposal uses a literature review approach to achieve the research objectives by systematically identifying, selecting, and synthesizing recent peer-reviewed studies on anomaly detection techniques for smart IoT environments. The review focuses on approaches published between 2024 and 2025 and emphasizes detection performance, deployment feasibility, robustness, privacy, and explainability.

Search strategy and sources

Relevant studies are collected from reputable academic sources and digital libraries (e.g., IEEE Xplore, SpringerLink, ScienceDirect, MDPI, and Google Scholar). The search uses combinations of keywords such as “IoT anomaly detection”, “intrusion detection IoT”, “one-class learning IoT”, “unsupervised anomaly detection”, “federated learning IDS”, “explainable AI IoT security”, and “concept drift IoT”.

Inclusion and exclusion criteria

Studies are included if they:

1. Address anomaly or intrusion detection in IoT networks or IoT data streams.
2. Propose, evaluate, or review machine learning/deep learning methods relevant to IoT security.
3. Report evaluation results, methodological insights, or deployment considerations.
4. Are peer-reviewed and published in the target timeframe.

Studies are excluded if they:

1. Focus on non-IoT contexts without relevance to IoT constraints or traffic characteristics.
2. Lack sufficient methodological detail or credible evaluation evidence.
3. Are non-peer-reviewed or purely opinion-based.

Selection and synthesis process

After collecting studies, titles and abstracts are screened to remove irrelevant papers, followed by full-text screening to confirm eligibility. For each included paper, key information is extracted,

including dataset and evaluation setting, detection methodology, reported metrics, and limitations. The extracted information is then synthesized into narrative sections (Summary, Critical Analysis, Connections, Conflicts) and organized into a synthesis matrix to support structured comparison.

Expected outcomes

This research proposal is expected to produce:

1. A structured synthesis of recent anomaly detection techniques for smart IoT environments, highlighting dominant approaches such as deep learning, unsupervised learning, hybrid methods, and privacy-aware federated learning.
2. A comparative understanding of trade-offs between detection effectiveness and real-world feasibility, with emphasis on constraints such as computational cost, model size, latency, scalability, and robustness.
3. Identification of major research gaps that reduce trust and deployability, including dataset dependency, limited real-device validation, concept drift challenges, explainability limitations, and security risks in distributed learning.
4. Practical research directions for developing more trustworthy IoT anomaly detection solutions that are lightweight, drift-aware, explainable, privacy-preserving, and resilient to adversarial behaviors.

Gantt chart

Task / Week	Week 1 (15–21 Nov 2025)	Week 2 (22–28 Nov 2025)	Week 3 (29 Nov–5 Dec 2025)	Week 4 (6–12 Dec 2025)	Week 5 (13–19 Dec 2025)	Week 6 (20 Dec 2025) Submission
Confirm title, scope, and objectives						
Collect recent literature (2024–2025)						
Screen papers (titles/abstracts) and shortlist						
Full-text reading and final paper selection						
Extract key information (methods/results/limits)						
Draft Chapter 1 (Introduction)						
Draft Chapter 2 (Literature review + synthesis)						

Build synthesis matrix and refine analysis						
Draft Chapter 3 (Methodology + expected outcomes)						
Final editing, formatting, and references						

References

Albanbay, N., Tursynbek, Y., Graffi, K., Uskenbayeva, R., Kalpeyeva, Z., Abilkaiyr, Z., & Ayapov, Y. (2025). Federated learning-based intrusion detection in IoT networks: Performance evaluation and data scaling study. *Journal of Sensor and Actuator Networks*, 14(4), 78. <https://doi.org/10.3390/jsan14040078>

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(1), 112. <https://doi.org/10.1140/epjqt/s40507-025-00414-6>

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>

Chu, R., Jin, P., Qiao, H., & Feng, Q. (2024). Intrusion detection in the IoT data streams using concept drift localization. *AIMS Mathematics*, 9(1), 1535–1561. <https://doi.org/10.3934/math.2024076>

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>

Misrak, S. F., & Melaku, H. M. (2025). Lightweight intrusion detection system for IoT with improved feature engineering and advanced dynamic quantization. *Discover Internet of Things*, 5, Article 97. <https://doi.org/10.1007/s43926-025-00203-8>

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>

Sharma, B., Sharma, L., Lal, C., & Roy, S. (2024). Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach. *Expert Systems with Applications*, 238, Article 121751. <https://doi.org/10.1016/j.eswa.2023.121751>

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>