Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

AI-Driven Anomaly Detection in IoT-Enabled HVAC and Water Heating Systems

Vignesh Alagappan

Sr. Manager, Ecosystem Engineering,
Rheem Manufacturing, 1115 Northmeadow Parkway, Suite 100, Roswell, GA 30076
Vignesh.alagappan@rheem.com

Abstract:
As buildings evolve into intelligent, connected ecosystems, Heating, Ventilation, and Air Conditioning (HVAC) systems — along with water heating infrastructure — are becoming increasingly IoT-enabled. These systems generate continuous streams of sensor data that can be harnessed to ensure energy efficiency, occupant comfort, and operational reliability. However, identifying performance degradation or faults within these complex, multi-component systems remains a challenge.

This paper explores an AI-driven approach for real-time anomaly detection in IoT-enabled HVAC and water heating systems. By leveraging machine learning (ML) and advanced data analytics, the proposed framework identifies abnormal patterns, predicts potential failures, and facilitates proactive maintenance — enabling energy savings, system longevity, and sustainability.

Keywords: IoT, HVAC systems, anomaly detection, machine learning, predictive maintenance, smart buildings, water heating, energy efficiency, digital twin, cybersecurity.

1. INTRODUCTION

1.1 Background

Modern HVAC and water heating systems integrate a wide range of IoT sensors, including temperature, pressure, flow rate, and vibration sensors, that continuously monitor system health [5]. While traditional rule-based monitoring can detect threshold breaches, it fails to capture complex, multi-variable anomalies caused by subtle degradation or component interactions [6].

AI and ML models, trained on large-scale operational datasets, can learn the normal behavior of systems and identify deviations dynamically [4], [10]. These deviations, when correlated with maintenance records and environmental data, can provide actionable insights for technicians and facility managers.

1.2 Motivation

The operation of HVAC and water heating systems accounts for **40–60% of a building's total energy consumption** [13]. Even minor inefficiencies, such as compressor wear, refrigerant leakage, or scaling in water heaters, can significantly increase energy usage [6], [13]. Early detection of such inefficiencies is vital to:

- Reduce maintenance costs and downtime.
- Improve equipment lifespan.
- Achieve sustainability and carbon reduction goals [3].

2. SYSTEM ARCHITECTURE

The proposed architecture for AI-driven anomaly detection consists of five interconnected layers, consistent with modern IoT edge–cloud reference models [8]

2.1 Device and Sensor Layer

IoT sensors embedded in HVAC and water heating systems capture metrics [5] such as:

- **Temperature:** inlet/outlet air or water temperature.
- **Pressure:** refrigerant pressure or pipe pressure.
- **Vibration and Sound:** motor imbalance, cavitation, or bearing wear.
- **Power Consumption:** Energy usage of the compressor, blower, or pump.

Sensor data is timestamped and metadata-tagged for downstream analytics.

2.2 Edge Gateway and Communication Layer

- Local gateways perform **edge preprocessing** — noise filtering, normalization, and time synchronization.
- Communication protocols: **MQTT, Modbus, BACnet, or Matter** (depending on system design) [7], [11].
- Encrypted transmission ensures data integrity and device trust via mutual TLS 1.2+ or certificate-based authentication.

2.3 IoT Cloud Platform (Secure Connectivity, Telemetry, Device Lifecycle Management)

Provides secure telemetry ingestion, device identity, over-the-air updates, and digital twin state management [8].

The IoT Cloud Platform serves as the backbone for security, orchestration, and data routing between field devices, edge gateways, and downstream analytics systems. It abstracts device heterogeneity, provides verifiable trust, and ensures that telemetry and control flows remain secure, scalable, and policy-governed throughout the device lifecycle [8], [12].

Capability	Description
Device Identity & Onboarding	Implements just-in-time or pre-provisioned enrollment using X.509 certificates, TPM/TEE-backed key storage, and PKI-based attestation [11], [12].
Secure Telemetry Ingestion	Uses MQTT/HTTPS over mTLS with role-based topic authorization, certificate pinning, and per-device policies [7].
Digital Twin / Device Shadow	Maintains a synchronized cloud-state model representing current status, last known telemetry, firmware version, and actuator state [8].
Device Lifecycle Management	Handles provisioning, ownership transfer, credential rotation, firmware rollback, remote decommissioning, and regulatory log retention [12].
Command & Control Plane	Enables secure downlink actions such as parameter tuning, soft resets, forced telemetry flush, and over-the-air patch execution [8].
Policy & Access Governance	Enforces fine-grained RBAC/ABAC, multi-tenant scoping, and audit logs to satisfy B2B, OEM, or field technician access models [7].
Telemetry Routing & Data Fan-out	Routes validated telemetry to different sinks — time-series DB, lakehouse, Kafka stream, alerting engine, or serverless functions.
Firmware & OTA Update Pipeline	Supports delta-patch distribution, signed image validation, staged/canary rollout, and post-update integrity attestation [2], [12].

2.4 Cloud Data Platform

- A **data lakehouse** integrates telemetry with metadata, operational logs, and maintenance records.
- Features extracted from raw data are stored in a **feature store** for model training and inference.
- Scalable compute resources enable periodic model retraining
- Supports Digital Twins and dashboards

2.5 AI/ML Layer

- Unsupervised and semi-supervised algorithms are used for anomaly detection:

Autoencoders — for reconstructing normal patterns and flagging deviations [10].
Isolation Forests — for outlier detection in multi-dimensional feature spaces [9].
LSTM networks — for detecting temporal anomalies in time-series data [10].

- Models are deployed as microservices within an MLOps framework for continuous monitoring and updates [2]

3. METHODOLOGY

Workflow: Data collection → preprocessing → feature engineering → model training → anomaly detection → automated actions [4], [12].

- **Data Collection:** Continuous acquisition of telemetry and operational data from IoT sensors.
- **Data Preprocessing:** Noise removal, missing value imputation, normalization, and synchronization.
- **Feature Engineering:** Domain-specific features like compressor cycling frequency, water temperature delta, and energy efficiency ratio (EER).
- **Model Training:** Using historical data to learn normal operational signatures.
- **Anomaly Detection:** Real-time inference to detect deviations; adaptive thresholds based on contextual parameters (ambient temperature, load conditions).
- **Alerting and Action:** Integration with building management systems (BMS) to trigger alerts or maintenance tickets

Domain features: compressor cycling frequency, delta-T, energy efficiency ratio (EER), pressure oscillation, and vibration FFT signatures [5], [6].

4. CASE STUDY: SMART BUILDING DEPLOYMENT

A pilot deployment was conducted in a **commercial facility** with 20 HVAC units and 15 water heating systems connected to an IoT platform.

Key outcomes:

- 22% reduction in unplanned maintenance incidents.
- 15% improvement in overall energy efficiency.
- Detection of early-stage compressor failure 2 weeks before actual breakdown.

Similar to results reported in [6].

5. CYBERSECURITY AND TRUST CHAIN

Ensuring data authenticity and model integrity is critical.

- **Device Identity and Certificates:** Each IoT device is issued a **Device Attestation Certificate (DAC)** by a trusted CA is aligned with NIST, ETSI, and Matter security frameworks [2], [7], [11], [12]
- **SDK Signing:** Edge SDKs are signed using **RSA-4096/ECC-P384** with SHA-256 for integrity verification [2], [7].
- **Secure Communication:** TLS 1.3 and certificate pinning ensure trusted connections between devices and the cloud [2], [7].
- **Model Trust:** Model versions are hashed and signed to prevent tampering.

6. CHALLENGES AND FUTURE WORK

Model drift, edge execution constraints, and cross-protocol interoperability have been widely documented in IoT AI deployments:

Challenge	Description	Future Direction
Data Quality	Sensor drift, noise, or missing data affect accuracy.	Use self-calibrating models and data validation pipelines.
Model Drift	Changing system behavior over time.	Implement continual learning and feedback loops.
Edge Deployment	Resource constraints for on-device inference.	Optimize models via pruning or quantization.
Interoperability	Diverse IoT protocols and legacy systems.	Standardize through OPC-UA, Matter, or BACnet integration.

7. CONCLUSION

AI-driven anomaly detection transforms HVAC and water heating systems from reactive to proactive assets, enabling them to operate more efficiently and effectively. By combining IoT data, ML models, and secure infrastructure, organizations can minimize downtime, optimize energy use, and move toward autonomous building operations. The integration of predictive intelligence with secure, scalable data frameworks marks the next evolution in sustainable facility management [4].

REFERENCES:

[1] ASHRAE, *Guidelines for Building Energy Performance Benchmarking*.

[2] NIST, "Building Secure Microservices-based Applications Using Service-Mesh Architecture," Special Publication 800-204A, 2020.

[3] ISO, "ISO 50001: Energy Management Systems," 2018.

[4] IEEE IoT Journal, "AI in HVAC fault detection and diagnosis: A systematic review," 2023.

[5] S. Katipamula and M. Brambley, "Methods for Fault Detection, Diagnostics, and Prognostics for Building Systems -- A Review," *HVAC&R Research*, 2005.

[6] F.Zhang, N.Saeed, P.Sadeghian, "Deep learning in fault detection and diagnosis of building HVAC systems: A systematic review with meta-analysis", 2023

[7] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, 2018.

[8] Microsoft Azure, "IoT Reference Architecture for Secure Device Connectivity," 2023.

[9] F. T. Liu et al., "Isolation Forest," *IEEE ICDM*, 2008.

[10] P. Malhotra et al., "LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection," arXiv:1607.00148, 2016.

[11] ETSI, "EN 303 645: Cyber Security for Consumer IoT Devices," 2020.

[12] Connectivity Standards Alliance, *Matter Device Library Specification*, 2023.

[13] "Energy Efficiency & Cost Savings for Building HVAC Systems," 2021.