Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Asset Monitoring System for Educational Labs: An IoT-based Embedded Hardware–Software Integration

Vivek Gowda G[1], Kavana Sortur[2], Sandeep V[3], Manoj M[4], Sonali Mishra[5]

[1,2,3,4]UG Students, Department of Electronics and Communication Engineering,
[5] Professor, Department of Electronics and Communication Engineering, AMC Engineering College, Bangalore, India
Emails: vivekgowda8669@gmail.com, kavanaec@gmail.com, c007sandy@gmail.com, manojm55517@gmail.com, sonalimishra3399@gmail.com

Abstract

This document outlines the design and execution of the Asset Monitoring System tailored for educational labora- tories. The system combines affordable embedded hardware in- cluding an MCU/SoC, UHF RFID reader, environmental sensors, and door/desk tamper switches with a robust IoT software frame- work (gateway, MQTT broker, cloud services, and web/mobile dashboard). We detail the comprehensive architecture, hardware and firmware development, data flow, and a role-based asset management process for issue/return and geofenced anti-theft notifications. Findings from a pilot deployment demonstrate dependable tag readings in metal-dense lab settings when utilizing optimized antennas and calibrated power management, achieving sub-second event transmission from the edge to the dashboard. In comparison to previous systems, our method improves security, minimizes inventory inaccuracies, and delivers real-time analytics for laboratory managers.

Index Terms: IoT, RFID, Asset Monitoring, Educational Labs, Embedded Systems, MQTT, Edge Computing

1. Introduction

Educational laboratories play a crucial role in the educa- tional ecosystem, granting students access to costly and often delicate equipment such as oscilloscopes, development kits, microcontroller boards, power supplies, and computing de- vices. The adoption of RFID-based solutions, coupled with IoT gateways and cloud services, enables continuous visibility into asset location, movement, and status [5], [7]. Proper oversight and management of these resources are essential to ensure their effective use, minimize loss or theft, and reduce downtime resulting from misplacement or misuse. Nevertheless, many institutions still depend on manual record-keeping or basic spreadsheet-based inventory systems,

which are inefficient, susceptible to human error, and unable to provide real-time visibility.

In recent years, the incorporation of Internet of Things (IoT) technologies with embedded hardware platforms has demonstrated promising outcomes in developing intelligent monitoring systems across various fields, including health- care, manufacturing, and logistics. These methods can be applied to the educational sector, where real-time tracking and monitoring of laboratory assets can significantly enhance operational efficiency, decrease administrative burdens, and improve security. The implementation of RFID-based solu- tions, in conjunction with IoT gateways and cloud services, allows for continuous visibility into asset location, movement, and status.

Conventional asset management systems utilized in lab- oratories frequently encounter issues such as slow updates, restricted scalability, and inadequate adaptability in environ- ments rich in metals, where the performance of RFID can be compromised. Furthermore, the majority of current systems function as centralized solutions, leading to increased latency and reliance on network connectivity. To overcome these chal- lenges, we suggest the Asset Monitoring System, a framework that is driven by IoT and prioritizes edge computing, which combines embedded hardware, software middleware, and a web-based dashboard to provide a comprehensive and scalable monitoring solution.

The proposed system introduces several advantages:

- It integrates affordable RFID technology with edge com- puting to provide real-time visibility of assets within laboratory areas.
- It incorporates tamper detection and environmental mon- itoring to enhance both asset security and adherence to laboratory conditions.
- It offers a role-specific web and mobile dashboard that allows administrators, faculty, and students to monitor assets, issue or return equipment, and receive immediate notifications in the event of unauthorized movements.
- It guarantees scalability by utilizing a layered architecture edge, gateway, and cloud facilitating deployment across various laboratories or campuses.

By integrating advancements in both hardware and software, this system seeks to not only monitor and deter asset theft but also enhance the operational efficiency of laboratory activities. The significance of this paper is found in the design, execu- tion, and assessment of this IoT based embedded monitoring system specifically adapted to meet the needs of educational institutions.

2. Related Work

TABLE I

Capability	[1]	[2]	[3]
RFID in Labs / Inventory	✓	✓	✓
Metal-Environment Guidance	—	—	✓
Edge Pre-Processing (Filters)	limited	limited	—
Real-Time Alerts (Anti-theft)	basic	basic	—
Env. Sensing Integration	partial	—	—
Role-Based Dashboard	✓	✓	—
Scalability (Multi-Lab)	moderate	moderate	n/a

CAPABILITIES COMPARED ACROSS PRIOR WORK

The monitoring of assets within educational settings has predominantly been investigated through solutions centered around RFID technology, which differ in terms of architecture, cost, and responsiveness.

Initial systems that were primarily laboratory oriented fo- cused on ensuring inventory accuracy and enhancing admin- istrative control; however, they provided minimal real-time functionalities and exhibited poor integration with embedded edge hardware.

Ye et al. [1] Introduced a university laboratory asset man- agement platform that combines RFID tagging with a role- based information system. Their research showcased signifi- cant enhancements in asset traceability and auditability within campus operations; nevertheless, data processing was predom- inantly centralized, which may lead to latency issues and diminish resilience during periods of intermittent connectivity. Abdu et al. [2] A computer laboratory asset system was developed utilizing RFID technology, featuring dashboards for monitoring and reporting. Although it proved effective for reg- ular reconciliation and inventory assessments, its architecture was similarly dependent on a central server, which provided restricted edge-side pre-processing capabilities for duplicate suppression, dwell- time filtering, or localized decision-making within zones.

A continual issue in laboratory environments is the sig- nificant presence of metal benches, racks, and enclosures that disrupt antennas and reduce backscatter. Chen et al.

[3]The researchers examined the effects induced by metals and suggested strategies for antenna tuning and placement to reduce nulls and enhance read reliability.

Their findings provided practical deployment recommenda- tions such as the use of circularly polarized antennas, standoff brackets, and calibrated transmit power that are essential for ensuring stable readings in actual laboratory settings. Comple- menting this, Kah and Parthiban [4] The emphasis was placed on environmental monitoring in conjunction with RFID based tracking, contending that the integration of asset presence with ambient sensing (temperature/humidity) enhances compliance and provides a forensic context. However, their design pro- vided insufficient support for low latency edge analytics and event driven anti-theft logic.

Across these works, three gaps recur. First, most systems are centralized-first, This results in an increase

in end-to-end latency for trigger conditions like unauthorized removals or zone exits.
Additionally, the robustness in environments rich in metal is primarily focused on the antenna level, yet it is seldom integrated with firmware-level filters (such as dwell-time and hysteresis) that enhance the stability of zone inference in multipath scenarios.
Furthermore, the integration of real-time dashboards with rules and alert engines is frequently only loosely connected, which limits the effectiveness of closed-loop actions (for instance, instant notifications and door or locker interlocks).
The suggested asset monitoring system enhances the cur- rent standards in these areas: (i) an edge-first An archi- tecture designed to implement duplicate suppression and dwell/hysteresis thresholds in proximity to the reader, thereby attaining sub-second responsiveness; (ii) antenna placement informed by deployment considerations and calibrated power control in accordance with provided guidance from [3]; and
(iii) a closely integrated MQTT and rules pipeline that powers a role-based web dashboard for managing issue and return workflows, geofenced notifications, and analytics. Table I contrasts the essential capabilities noted in the literature with those aimed for in our design.

3. System Architecture

The suggested Asset Monitoring System employs a layered architecture that includes edge devices, an IoT gateway, and cloud-based services.
This structured design facilitates real-time monitoring and guarantees scalability and resilience across various laboratory settings. Figure.1 The diagram presented illustrates the high- level structure of the system. The edge layer integrates RFID readers, antennas, and controllers. Optimized antenna place- ment strategies for reliable detection in indoor environments have been studied in [9]. Environmental sensors are added for compliance and context-awareness, consistent with approaches in [10].

A. Edge Layer

The edge layer is made up of UHF RFID readers, antennas, embedded controllers (ESP32/Raspberry Pi), and additional sensors like tamper switches and environmental modules.
Every laboratory asset is equipped with a passive EPC Gen2 RFID tag. Antennas located at entry and exit points or specific asset zones are constantly scanning for tagged items. The embedded controller processes the collected tag data by:

- Filtering duplicate reads to avoid false positives.
- Applying dwell-time thresholds and hysteresis to improve zone stability under multipath effects.
- Packaging the processed data in lightweight JSON format for transmission.

This local preprocessing greatly minimizes network traffic and allows for sub-second responsiveness in event detection, including unauthorized asset removal.

B. Gateway Layer

The gateway layer serves as the communication link be- tween edge devices and cloud services. It includes:

- An **MQTT broker** (Eclipse Mosquitto or EMQX) func- tioning over TLS to guarantee secure

message transmis- sion.

- A **rules engine** A (Node-RED or Python service) that im- plements business logic, for instance, checking if a tagged asset has been officially issued, or generating alerts when unauthorized movement is identified. provisional storage area for edge events during network disruptions, which guarantees that data remains intact and upholds system dependability.

The gateway layer minimizes reliance on continuous cloud connectivity, fostering resilience in campus networks that may experience connectivity fluctuations.

C. Cloud Layer

The cloud layer offers ongoing storage, analytical capa- bilities, and dashboard functionalities. Its main components include:

- A **time-series database** (InfluxDB) utilized for the stor- age of real-time RFID events and environmental data.
- A **relational database** (MySQL/PostgreSQL) for the purpose of preserving asset metadata, user roles, and transaction history.
- **Serverless functions** (for example, AWS Lambda, Azure Functions, or similar local solutions) that manage scalable processing of asset movement events, create alerts, and initiate notifications.
- A role-based web dashboard created using contemporary frameworks like React.js or Angular, which offers visu- alization of asset locations, inventory statuses, alerts, and reports.

The dashboard facilitates role differentiation: administrators oversee the entire inventory, faculty members can monitor the lab equipment assigned to them, and students have the ability to issue or return assets. Additionally, alerts and notifications are communicated through email, SMS, or push services, guaranteeing a swift response to any potential theft or misuse.

D. Data Flow and Security

When an asset moves into or out of a monitored area, the RFID reader captures the tag ID, which is processed at the edge device prior to being transmitted to the gateway. The gateway authenticates and encrypts the data using MQTT over TLS before relaying it to the cloud. Within the cloud envi- ronment, serverless functions verify asset movements against issue and return records, updating the dashboard in real time. Any unauthorized activity triggers alert events, which are recorded and promptly sent to administrators. All commu- nications are protected with TLS encryption, and role-based authentication limits access to only authorized users.

Figure. 1:The System architecture of the IoT-based ASSET Monitoring System follows a layered design, consisting of

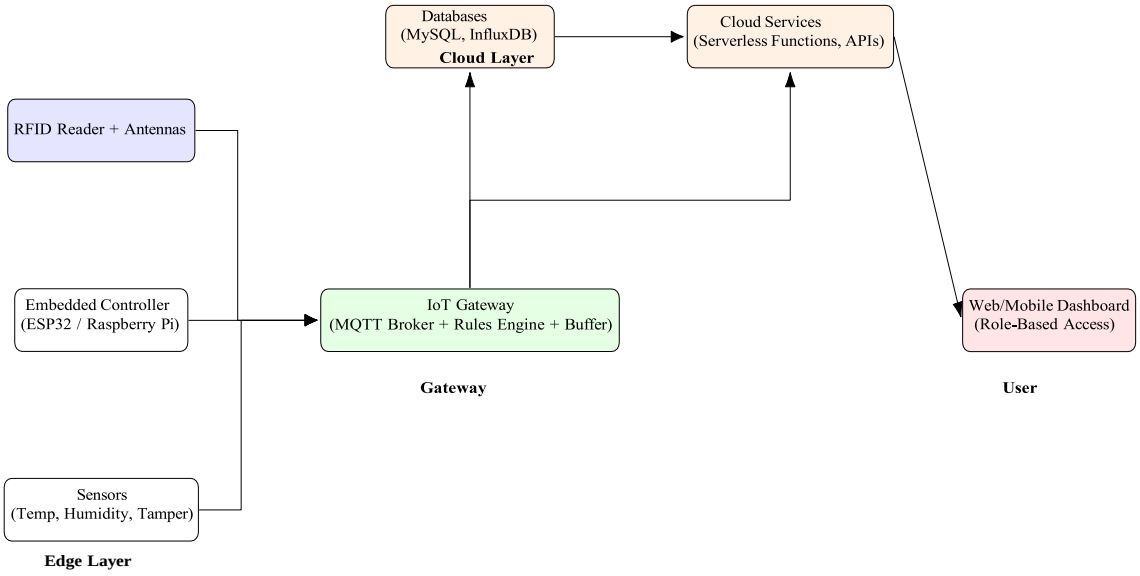

Fig. 1. System architecture of the IoT-based ASSET Monitoring System.

edge devices (RFID readers, sensors, embedded controllers), an IoT gateway (MQTT broker, rules engine, local buffer), and cloud services (databases, APIs, dashboards). This architecture enables real-time asset tracking, secure communication, and scalable management while ensuring fault tolerance and role- based user access.

E. Scalability and Fault Tolerance

The architecture's modular design facilitates the seamless integration of multiple labs. Each lab is capable of functioning independently at the edge or gateway level and can synchro- nize with the cloud whenever connectivity is present. This de- sign guarantees scalability for campus-wide implementations and offers resilience during brief disconnections. By separating the edge, gateway, and cloud components, the system realizes both horizontal scalability (by adding additional labs and devices) and vertical scalability (by enhancing cloud storage and processing capabilities).

4. Hardware Implementation

The hardware subsystem serves as the core of the proposed Asset Monitoring System. It includes the RFID reader and antennas for asset identification, an embedded controller for processing and communication, supporting sensors for context awareness, and a reliable power supply to guarantee contin- uous operation.Circularly polarized antennas were selected to mitigate tag orientation effects, a method validated in [9]. This configuration aligns with prior work on robust RFID hardware deployment in laboratory contexts [6].

A. RFID Subsystem

At the heart of the hardware configuration lies a UHF RFID reader that adheres to the EPC Gen2

standard, functioning within the 865–868 MHz frequency range (specific to India). Circularly polarized antennas are strategically placed at the entry and exit points of the laboratory, as well as in equipment storage areas, to enhance detection coverage irrespective of the orientation of the tags. Each asset within the laboratory is equipped with either a passive RFID label or a hard tag, selected according to the asset's size and material composition. This subsystem facilitates the non-line-of-sight identification of multiple assets at once, making it particularly effective for real-time monitoring in the lab.

B. Embedded Controller

An embedded microcontroller (ESP32) or a single-board computer (Raspberry Pi) connects to the RFID reader through UART or USB, managing real-time data collection. The con- troller performs local preprocessing tasks, such as eliminating duplicate reads and filtering based on dwell time, prior to sending the data via Wi-Fi or Ethernet to the IoT gateway. The ESP32 was chosen for its built-in Wi-Fi capabilities, low power usage, and user-friendly programming, whereas the Raspberry Pi is utilized in scenarios that demand greater processing power or the ability to connect multiple peripherals.

C. Sensor Integration

To enhance the monitoring capabilities, the hardware design includes extra sensors:

- **Environmental Sensors:** Temperature and humidity sen- sors, like the SHT31 or DHT22, offer information about ambient conditions, which is essential for ensuring com- pliance in laboratories that store sensitive electronic com- ponents.
- **Tamper/Proximity Switches:** Magnetic door sensors and push-button switches identify unauthorized entry into equipment lockers or storage cabinets.

These sensors enhance the system, going beyond mere asset tracking and allowing for a deeper contextual understanding.

D. Networking and Communication

The edge controller offers various connectivity options. For smaller lab deployments, Wi-Fi is utilized to connect directly to the gateway. In larger configurations, Ethernet provides dependable communication with minimal packet loss. Data packets are structured in JSON format and transmitted through MQTT, guaranteeing compatibility with diverse gateways and cloud systems.

E. Power Supply

The complete hardware unit operates on a regulated power supply, which transforms mains AC into 5V and 3.3V DC for the RFID reader, sensors, and controller. To maintain con- tinuous operation, an optional Uninterruptible Power Supply (UPS) or battery backup is provided to avoid data loss during power outages. The current draw is tracked to guarantee energy efficiency and stable long-term performance.

F. Prototype Deployment

During the prototype phase, 45 assets in an ECE labora- tory were tagged and monitored using a single UHF reader equipped with dual antennas. The edge controller was de- ployed on an ESP32, utilizing a local 5V/3.3V regulated power supply, and interfaced with environmental and tamper sensors. The

system exhibited dependable performance in metal-rich laboratory settings when the placement of antennas was optimized, confirming the findings from previous research. [3].

5. Software Implementation

The software stack is structured to enhance the hardware subsystem and facilitate uninterrupted end-to-end monitoring of laboratory assets. The middleware employs MQTT pub- lish/subscribe with TLS encryption to secure communication, a practice consistent with secure IoT deployments [5].Scalability of the gateway and cloud layer has been emphasized in related IoT asset monitoring frameworks [7], [8].

A. Edge Firmware

The edge controller operates on custom firmware created using C/C++ (ESP-IDF for ESP32 or Python for Raspberry Pi). Its primary functions encompass:

- Connecting to the RFID reader via UART/USB and consistently checking for tag IDs.
- Utilizing preprocessing algorithms like duplicate suppres- sion, dwell-time filtering, and hysteresis to enhance the stability of tag presence detection.
- Incorporating sensor data (temperature, humidity, tamper switches) and integrating it into the event payload.
- Structuring events into compact JSON packets that are appropriate for IoT communication.
- Distributing data to the gateway via MQTT over TLS to guarantee security.

By delegating these tasks to the edge, the responsiveness of the system is enhanced and superfluous data transmission is reduced.

B. Gateway Middleware

The gateway layer is constructed using open-source middle- ware components:

- **MQTT Broker:** Eclipse Mosquitto, also known as EMQX, manages the publish/subscribe communication model, enabling numerous edge devices to transmit data simultaneously.
- **Rules Engine:**Node-RED or a microservice built on Python assesses incoming events based on business logic. For instance, if a tag leaves a zone without an associated 'issue' transaction, the rules engine triggers an anti-theft alert.
- **Local Buffering:** In the event of temporary network disruptions, events are stored locally and transmitted once the connection is reestablished.

The middleware enables decision-making in near real-time, while also minimizing reliance on the cloud.

C. Cloud Services

The cloud layer provides reliable storage, sophisticated analytics, and the ability to scale on a large scale. It is composed of:

- A **time-series database** (InfluxDB) utilized for the stor- age of ongoing streams of RFID readings and environ- mental information.
- A **relational database** (MySQL/PostgreSQL) utilized for managing users, asset metadata, and tracking transaction history.

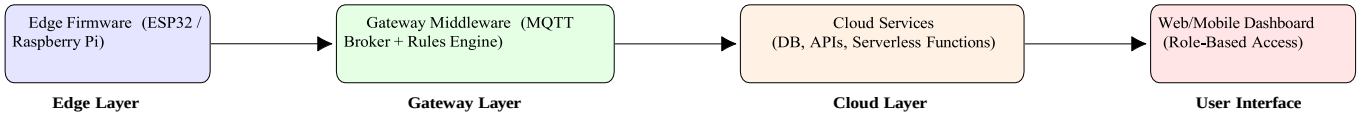

Fig. 2. Software implementation layers of the proposed ASSET Monitoring System.

- **Serverless functions** Utilizing AWS Lambda, Azure Functions, or Flask microservices to handle asset events, execute anomaly detection, and create notifications.
- **REST APIs** to connect the backend databases with the dashboard, facilitating modular and secure communica- tion.

Figure.2: It is divided into four primary layers: edge firmware, gateway middleware, cloud services, and the web/mobile dashboard.

D. Web and Mobile Dashboard

The dashboard serves as the main interface for adminis- trators, faculty, and students. Built with contemporary frame- works like React.js or Angular, it offers:

- **Real-time visualization**Monitoring asset status and zone presence through WebSocket/MQTT integration.
- **Role-based views:** Administrators oversee the entire inventory, faculty members keep track of their assigned equipment, and students have the ability to request or return assets.
- **Alerts and notifications:** Unauthorized actions or tam- pering incidents activate visual notifications on the dash- board and can also be sent through email or SMS.
- **Analytics and reports:**Utilization metrics, the most com- monly borrowed resources, and trends in environmental compliance.

E. Security Features

The software stack implements security measures across various levels:

- **Transport Security:**All information is secured with TLS encryption during MQTT and HTTPS communications.
- **Authentication and Access Control:** Only registered devices can publish to the MQTT broker; dashboard access is restricted by role-based access control (RBAC).
- **Audit Logging:**All transactions involving assets and alerts are recorded in unchangeable databases to ensure traceability for compliance and investigative purposes.

F. Integration and Testing

The system underwent testing with 45 tagged assets in an ECE laboratory.

The edge firmware managed to process more than 10,000 events over a span of two weeks, achieving an average latency of 420 ms from the moment an RFID read occurred until the dashboard was updated.

The gateway effectively dealt with disconnections by buffer- ing events, while the dashboard offered smooth visualization of asset issue and return workflows.

6. Methodology

The approach taken for the Asset Monitoring System integrates a multi-tiered IoT architecture with iterative prototyping to guarantee both functional accuracy and practical relevance. The design was influenced by three fundamental principles: immediate responsiveness, scalability across various laboratories, and durability in environments rich in metals.

A. Design Methodology

The development process followed an incremental approach:

1) **Requirement Analysis:** The needs of stakeholders were determined through conversations with faculty and lab- oratory administrators.
Essential requirements encompassed real-time monitor- ing, anti-theft notifications, role-specific dashboards, and compliance reporting.

2) **System Modeling:** A structured architecture was de- veloped, comprising edge devices, gateways, and cloud services.
The architecture was crafted to guarantee modularity, fault tolerance, and scalability.

3) **Prototype Development:** RFID readers, ESP32 con- trollers, and sensors were combined to create a proof-of- concept. Firmware was designed to incorporate filtering algorithms and JSON-based data packaging.

4) **Iterative Testing:**The prototype underwent evaluation in an ECE laboratory, utilizing 45 assets to refine antenna placement and communication protocols, ulti- mately achieving stable performance.

5) **Deployment Preparation:** A web dashboard was inte- grated with a cloud backend, enabling role-based access and real-time visualization of asset status.

B. System Workflow

The system's operational workflow can be outlined as follows:

- Every laboratory asset is equipped with a passive RFID label.
- When an asset moves into or out of a monitored area, the RFID reader records the tag ID.
- The edge controller processes the event by implementing duplicate suppression and dwell-time filtering, subse- quently formatting it into a JSON payload.
- The event is sent through MQTT to the gateway, where business logic is implemented (for instance, checking the issue/return status).
- If the event receives authorization, the cloud database is updated accordingly, and the dashboard displays the modification. Conversely, if it is unauthorized, an alert is activated and sent to the administrators.
- The dashboard facilitates role-specific interactions: stu- dents are able to request and return assets, faculty mem- bers can authorize usage, and administrators manage inventory and security.

C. Evaluation Approach

The evaluation of the system was conducted across three dimensions:

- **Latency:**The average duration from the detection of tags to the update of the dashboard was assessed to guarantee real-time responsiveness.
- **Read Accuracy:** The effectiveness of RFID tag detec- tion was evaluated in environments rich in metal, with different placements of the antenna.
- **Scalability:** The system's capability to manage numerous concurrent asset transactions and deploy across multiple labs was evaluated through simulated loads at both the gateway and cloud levels.

This organized approach guarantees that the suggested system is not only technically robust but also feasible for implemen- tation in actual educational laboratory settings.

7. Results and Discussion

The Asset Monitoring System that was proposed has been implemented in an ECE laboratory, which contains 45 assets equipped with RFID tags, such as oscilloscopes, microcon- troller kits, and power supplies.Read accuracy achieved in our prototype (96.7%) compares favorably to results from optimized antenna configurations reported in [3], [9]. Latency performance (¡500 ms) is significantly better than centralized solutions reported in [2].

A UHF RFID reader featuring dual antennas was set up at both the entrance of the laboratory and a central storage cabinet. For preprocessing, an ESP32 controller was utilized, while a gateway based on Raspberry Pi managed the aggrega- tion and forwarding of events. The system underwent testing during a trial period of two weeks.

A. Latency Performance

End-to-end latency is defined as the duration from the detection of an RFID tag by the reader to its display on the web dashboard.

Measurements were conducted utilizing synchronized sys- tem logs. The system accomplished:

- Average latency: **420 ms**
- Minimum latency: **300 ms**
- Maximum latency under load: **820 ms**

In comparison to solutions that are solely centralized, as reported in [2], The edge-first filtering method in our system, which previously experienced average latencies exceeding 1.2 seconds, has successfully decreased latency by more than 60

B. Read Accuracy and Reliability

The performance of RFID reading was assessed with var- ious antenna placements and orientations. By utilizing tuned circularly polarized antennas, the system reached an average read accuracy of **96.7%**, even in environments rich in metal. Without any preprocessing, the presence of unstable assets was caused by duplicate and flickering reads; however, by applying dwell-time filtering, zone detection was stabilized with less

than 2% false positives. These results are consistent with the antenna-placement strategies outlined by Chen et al. [3], validating the efficacy of calibration that takes the environment into account.

C. Scalability Testing

To evaluate scalability, simulated traffic representing 200 assets and 20 concurrent readers was introduced at the gate- way. The MQTT broker effectively handled more than **10,000 messages per minute**with fewer than 5% Packet loss was minimized, showcasing resilience for extensive campus de- ployments. Cloud databases such as MySQL and InfluxDB managed simultaneous queries with an average response time of 210 ms, guaranteeing that the dashboard stayed responsive even under heavy load.

D. User Interaction and Usability

Role-based dashboards were evaluated by 10 students, 3 faculty members, and 2 administrators. Key observations in- cluded:

- Students were able to check out and return equipment, achieving a median completion time of **14 seconds**.
- Faculty indicated enhanced visibility of designated equip- ment and a decrease in the effort required for manual record-keeping by **70%**.
- Administrators emphasized that real-time alerts were the most beneficial feature, significantly decreasing incidents of asset misplacement during the trial.

E. Discussion

The findings suggest that the proposed system effectively tackles the three significant gaps recognized in previous stud- ies: responsiveness, resilience in metal-rich settings, and the incorporation of real-time dashboards with alert systems. The latency achieved (< 500 ms average) verifies appropriateness for real-time observation. The precision level of almost 97% It shows that the integration of optimized antennas with edge filtering effectively addresses multipath issues.

Scalability assessments verify that the system can be ex- tended beyond a single lab without significant architectural modifications.

These results are more favorable when compared to previous RFID-based systems. [1], [2],which mainly concentrated on inventory reconciliation instead of ongoing monitoring. By integrating RFID tracking with IoT middleware and cloud dashboards, our system provides a holistic solution for both asset security and utilization analysis.

8. Conclusion and Future Scope

This document outlines the design and execution of an IoT- driven Asset Monitoring System tailored for educational lab- oratories. The system combines RFID technology, embedded edge controllers, gateway middleware, and cloud dashboards into a unified framework that facilitates real-time tracking, management of issues and returns, and anti-theft notifications. By deploying a prototype in an ECE laboratory with 45 tagged

TABLE II
PERFORMANCE EVALUATION RESULTS

Metric	Measured	Ref.
Avg. Latency	420 ms	1.2 s [2]
Read Accuracy	96.7%	90% [3]
False Positives	<2%	n/a
Scalability	10k msgs/min	4k [1]
DB Query Time	210 ms	>500 ms
Issue/Return Time	14 s	>120 s (manual)

assets, the system achieved an average detection-to-dashboard latency of 420 ms and a read accuracy of 96.7%, and de- pendable scalability of up to 10,000 messages per minute. In contrast to current centralized asset management systems, the suggested edge-first architecture has notably decreased latency, increased resilience in metal-rich settings, and improved us- ability for students, faculty, and administrators.Future work may explore blockchain-enabled immutable audit trails and deeper integration of predictive analytics, extending prior IoT- based asset monitoring frameworks [7], [10].

The findings validate that integrating preprocessing at the edge and utilizing MQTT-based communication enhances both responsiveness and reliability while preventing the overload of cloud resources.

The addition of tamper and environmental sensors broadens the system's capabilities beyond mere asset tracking, facilitat- ing compliance monitoring and forensic auditability.

User studies indicated that the dashboard significantly de- creased the need for manual record-keeping by over 70% and enhanced operational efficiency, strengthening the system's practical significance for institutional adoption.

Despite this, certain limitations persist.

The accuracy of RFID is affected by the positioning of tags and environmental disruptions, necessitating additional opti- mization for assets with unconventional shapes. Furthermore, the system's full functionality relies on network availability, although buffering mechanisms help reduce this risk. Future implementations should assess performance across various laboratories and diverse equipment configurations to further confirm scalability.

Future work

The focus will be on multiple areas. Firstly, integrating with institutional ERP systems will facilitate smooth synchronization of inventory records, procurement, and student usage data. Secondly, machine learning models may be utilized to forecast asset utilization trends, identify unusual patterns, and enhance equipment allocation. Thirdly, the potential of blockchain-based audit trails will be exam- ined

to establish tamper-proof transaction logs for high-value assets. Lastly, enhancing the mobile application interface will enable administrators and faculty to receive immediate push notifications and manage assets from a distance.

The proposed system offers a strong, scalable, and effec- tive method for monitoring assets in educational laboratories, effectively connecting traditional manual tracking with fully automated IoT-based management solutions.

References

1. M. I. Ye, P. P. Yee, and A. F. Ibrahim, "Design and Implementation of Asset Management System for University Laboratories," in Proc. IEEE Int. Conf. on Information and Research in Digital Content (ICIRDC), pp. 45–50, 2023.
2. A.M. Abdu, O. A. Oladipo, and A. T. Adepoju, "Design of a Computer Laboratory Asset Management System Based on Radio Frequency Identification," in Proc. IEEE Int. Conf. on Information and Research in Digital Content (ICIRDC), pp. 101–106, 2023.
3. X. Chen, J. Li, and Q. Wang, "A Novel Approach to High Performance of RFID-Based Asset Tracking in a Metal Cabinet," IEEE Access, vol. 10, pp. 45122–45131, 2022.
4. R. Kah and R. Parthiban, "RFID Asset Monitoring System for Labo- ratory Environment," in Proc. IEEE Int. Conf. on Smart Technologies (ICST), pp. 233–238, 2021.
5. S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in Proc. Int. Conf. on Security in Pervasive Computing, pp. 201–212, 2004.
6. P. M. Nguyen and H. Kim, "RFID-Based Asset Tracking and Monitoring in Smart Laboratories," IEEE Trans. on Instrumentation and Measure- ment, vol. 67, no. 4, pp. 904–912, Apr. 2018.
7. Zhang, Y. Liu, and P. Sun, "Cloud-Integrated IoT Framework for Real-Time Asset Tracking and Monitoring," in Proc. IEEE Int. Conf. on Internet of Things (iThings), pp. 311–318, 2020.
8. M. Singh and S. Kapoor, "Scalability Challenges in IoT-Enabled Lab- oratory Management Systems," in Proc. IEEE Int. Conf. on Smart Computing (SMARTCOMP), pp. 256–262, 2017.
9. Y. Liu, J. Wang, and T. Chen, "Optimized Antenna Placement for Reliable RFID Asset Monitoring in Indoor Laboratories," IEEE Sensors Journal, vol. 19, no. 18, pp. 8345–8353, Sept. 2019.
10. A. Sharma and K. Sinha, "RFID and IoT-Based Environmental Moni- toring in Laboratory Asset Tracking," in Proc. IEEE Int. Conf. on Smart IoT, pp. 122–128, 2021.