BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

# LABSHIELD AI: A PRIVACYAWARE AIoT LABORATORY RISK INTELLIGENCE SYSTEM

**Zarrish Shaikh , Jiya Sharma , Snehal Thombare , Prof. Ankita Pokale (Guide)**

Department of Artificial Intelligence & Data Science Engineering Ajeenkya DY Patil School of Engineering, Pune, India

**Abstract**

Engineering laboratories contain electrical and electronic equipment that may be exposed to overheating, abnormal power consumption, unattended operation, unauthorized access, smoke or gas hazards, and other unsafe conditions. Conventional monitoring is often manual, reactive, and based on isolated sensor readings. This paper presents LabShield AI, a privacy-aware Artificial Intelligence of Things (AIoT) laboratory risk intelligence and decision-support architecture. The proposed system integrates temperature, humidity, power, occupancy, smoke/gas, laboratory access, and equipment-status information through an ESP32 edge controller. Sensor observations are buffered and transmitted through secure MQTT/TLS or HTTPS channels to a cloud/backend layer for validation, cleaning, normalization, and storage. Machine-learning components based on Random Forest or Decision Tree classification and Isolation Forest anomaly detection are proposed to analyze multi-parameter conditions. The system converts the analysis into a Laboratory Risk Score on a 0–100 scale with SAFE, WARNING, and CRITICAL states, and presents contributing factors and actionable recommendations through a web dashboard. Privacy-aware identifiers and role-based access control are incorporated to reduce unnecessary exposure of personal information. The architecture is motivated by recent research on AIoT laboratory monitoring, industrial predictive maintenance, IoT security, privacypreserving analytics, and IoT cybersecurity baselines [1]–[10]. The paper describes the system design, processing workflow, security model, and evaluation requirements. Since the supplied project material does not report measured experimental results, no performance values are claimed here; experimental validation is identified as necessary before publication as an empirical performance study.

**Keywords:** AIoT, Internet of Things, laboratory monitoring, risk intelligence, machine learning, anomaly detection, privacy, ESP32, MQTT, cybersecurity.

## INTRODUCTION

Engineering laboratories are shared environments containing electrical, electronic, and computing equipment that may operate under varying loads and usage patterns. The project specification identifies overheating, unattended equipment, unauthorized access, uncontextualized smoke/gas readings, manual interpretation of multiple sensor streams, and privacy risks in access records as important monitoring challenges. The proposed LabShield AI system addresses these challenges by combining sensing, edge processing, secure communication, machine learning, risk scoring, and dashboardbased decision support in a single architecture.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Recent work demonstrates the relevance of AIoT to laboratory monitoring. Qiang et al. proposed a BIM-AIoT framework for engineering laboratory monitoring and management, showing the potential of integrating IoT data with intelligent analysis for laboratory environments [1]. In a different setting, ExaMon-X demonstrated heterogeneous monitoring and AI-assisted predictive maintenance for industrial high-performance-computing systems [2]. These studies motivate the use of multi-source sensing and automated analysis, while leaving room for a lightweight laboratory-oriented architecture that combines physical risk monitoring, access information, privacy, and actionable recommendations.

Security and privacy are also central to IoT deployments. Ghaffari et al. reviewed machine- and deep-learning approaches for IoT security, including unauthorized access, spoofing, denial-of-service attacks, eavesdropping, and intrusion detection [3]. Rodríguez et al. surveyed ML/DL methods for privacy protection in IoT environments [4].

Digital-twin and wireless-sensor-network research further emphasizes data protection and integrity in distributed sensing environments [5], [6]. These findings support incorporating security and privacy from the system-design stage rather than treating them as optional dashboard features.

## PROBLEM STATEMENT

The core problem is the absence of an integrated, low-cost, privacyaware mechanism for continuously observing laboratory conditions and translating heterogeneous sensor observations into understandable risk information. A single temperature threshold, power reading, motion event, or smoke reading may not adequately represent the laboratory state. Context can be obtained by considering multiple parameters together, including occupancy, access, and equipment status.

LabShield AI therefore targets a multi-parameter decision-support workflow: sensor data → edge buffering → secure transmission → preprocessing and storage → ML/anomaly analysis → risk score → dashboard → recommendation. The system is intended to assist laboratory administrators and is not presented as a replacement for physical safety procedures or human judgment.

## III. OBJECTIVES

1. Design an AIoT architecture for laboratory environmental, equipment, power, occupancy, and access monitoring.
2. Collect and timestamp multi-sensor observations using an ESP32 controller.
3. Buffer observations at the edge and transmit them through encrypted MQTT/TLS or HTTPS channels.
4. Validate, clean, normalize, and store incoming observations in a structured backend.
5. Apply supervised classification and unsupervised anomaly detection to identify abnormal multi-parameter conditions.
6. Generate an explainable Laboratory Risk Score from 0 to 100 with SAFE, WARNING, and CRITICAL states.
7. Provide dashboard alerts, contributing factors, and natural-language recommendations.
8. Use pseudonymous identifiers and role-based access control to reduce unnecessary exposure of personal information.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

## RELATED WORK AND LITERATURE SURVEY

### A. AIoT Laboratory Monitoring

Qiang et al. presented "Integrating BIM and AIoT for Smart Engineering Laboratory Monitoring and Management," published in IEEE Internet of Things Journal in 2025 [1]. The work integrates BIM and IoT information for real-time indoor environmental-quality monitoring and prediction and uses computer-vision-based analysis. The study establishes a direct precedent for intelligent engineeringlaboratory monitoring. LabShield AI differs in scope by emphasizing a unified laboratory risk workflow involving environmental conditions, equipment/power state, access, privacy, anomaly detection, and recommendations.

### B. Predictive Maintenance and Heterogeneous Monitoring

Borghesi et al. developed ExaMon-X, a predictive-maintenance framework for automatic monitoring in industrial IoT systems [2]. The framework combines heterogeneous monitoring data with AI-based analytics and was evaluated on production HPC systems. Its industrial scale demonstrates the value of heterogeneous monitoring, but the architecture is more extensive than required for a small educational laboratory. LabShield AI adapts the general idea toward a lightweight ESP32-centered deployment.

### C. Machine Learning for IoT Security

Ghaffari et al. reviewed ML and DL approaches for IoT security and discussed threats such as unauthorized access, spoofing, denial-ofservice attacks, eavesdropping, and intrusion detection [3]. This literature supports the inclusion of secure communication, access control, and intelligent anomaly analysis in IoT architectures.

### D. Privacy Protection in IoT

Rodríguez et al. surveyed ML/DL approaches for privacy protection in IoT and highlighted privacy threats and ML-based mitigation approaches [4]. For laboratory deployments, privacy is particularly relevant when access events can indirectly reveal individual activity. LabShield AI therefore uses pseudonymous identifiers in the proposed data model and separates access permissions through RBAC.

### E. Digital Twin and Sensor-Data Security

Alhamam et al. reviewed cybersecurity issues in Digital Twin environments, including threats affecting data and connected systems [5]. Zhang et al. proposed a privacy- and integrity-preserving data aggregation scheme for wireless sensor networks using Digital Twin concepts and homomorphic fingerprinting [6]. These works reinforce the need for secure sensing and data handling, while LabShield AI deliberately uses a lighter security architecture suitable for an ESP32/cloud prototype.

### F. ML Methods Supporting the Proposed Design

Random Forest is a well-established ensemble of decision trees and is suitable as a candidate classifier for structured multi-parameter data [7]. Isolation Forest provides an unsupervised method for identifying unusual observations by isolating anomalies in feature space [8]. For explainability, SHAP provides feature-attribution values that can be used to describe how individual input variables contribute to a model

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

prediction [9]. These methods align with the project requirement for risk classification, anomaly detection, and explainable contributing factors.

**G. IoT Communication and Cybersecurity Baselines** MQTT 5.0 is an OASIS-standard lightweight publish/subscribe protocol designed for constrained IoT and machine-to-machine communication [10]. The proposed use of MQTT over TLS is consistent with the need for secure IoT communication. NIST's IoT cybersecurity baseline identifies capabilities including device identification, data protection, logical access control, software update, cybersecurity state awareness, and device security [11]. OWASP's IoT Top 10 also highlights insecure interfaces, insecure data transfer/storage, insufficient privacy protection, weak credentials, and insecure updates as recurring IoT risks [12].

## RESEARCH GAP

The literature indicates strong individual solutions for laboratory environmental monitoring [1], industrial predictive maintenance [2], IoT security [3], privacy protection [4], and secure distributed sensing [5], [6]. However, the project targets a combined workflow for an educational laboratory: (i) multi-parameter physical sensing, (ii) equipment and power context, (iii) occupancy and access events, (iv) ML-based risk classification and anomaly detection, (v) explainable 0– 100 risk scoring, (vi) privacy-aware identifiers and RBAC, and (vii) actionable recommendations in one lightweight architecture. The research contribution is therefore positioned as an integrated system design rather than a claim that any individual algorithm is novel.

## PROPOSED LABSHIELD AI ARCHITECTURE

### A. Sensing Layer

The sensing layer contains a DHT22 temperature/humidity sensor, ACS712 or INA219 power/current sensing, PIR motion sensing, RC522 RFID-based access sensing, and MQ-2 smoke/gas sensing. The monitored context also includes equipment status. The sensors are intended to operate concurrently so that the backend receives a multiparameter representation of the laboratory state.

### B. Edge Controller

An ESP32 development board acts as the primary edge controller. It receives sensor readings, timestamps them, and buffers them before transmission. Edge buffering provides a practical separation between physical sensing and cloud processing and can reduce the effect of short network interruptions.

### C. Secure Communication and Backend

The proposed communication path uses MQTT over TLS or HTTPS. MQTT is particularly relevant to constrained IoT communication because of its lightweight publish/subscribe model [10]. At the backend, incoming payloads are validated, cleaned, normalized, and stored. The proposed software stack includes Python with FastAPI or Flask, Firebase or an MQTT cloud broker, and Pandas/NumPy/scikitlearn.

### D. Machine-Learning Layer

The primary classification option is Random Forest or Decision Tree for NORMAL, WARNING, and CRITICAL classes. Random Forest provides an ensemble-based classification mechanism [7]. Isolation Forest is proposed as an additional unsupervised anomaly detector for observations that do not resemble

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

normal data distributions [8]. The final implementation should determine model hyperparameters and decision thresholds through validation data rather than assuming that the project-defined risk bands are statistically optimal.

## E. Risk Score and Decision Support

LabShield AI represents laboratory risk on a 0–100 scale. The project defines three operating bands: 0–30 SAFE, 31–60 WARNING, and 61–100 CRITICAL. The score is intended to summarize multiparameter analysis and model confidence. The dashboard presents the current state, contributing factors, trends, and a recommended action. These ranges are design requirements from the project and should be empirically validated before being presented as clinically, scientifically, or statistically optimized thresholds.

## F. Explainability

The system is designed to report contributing factors rather than only displaying a class label. SHAP is a suitable explainability framework because it assigns feature-attribution values to individual predictions [9]. For example, a final implementation could show which measured variables contributed most strongly to a warning or critical classification. The exact explanation method and model-specific SHAP implementation must be validated with the selected classifier.

### SYSTEM OPERATION

1. **Sensor Data Collection:** DHT22, ACS712/INA219, PIR, RC522, and MQ-2 collect laboratory observations.
2. **ESP32 Buffering:** The ESP32 receives, timestamps, and temporarily buffers the observations.
3. **Secure Transmission:** Sensor payloads are transmitted through MQTT/TLS or HTTPS.
4. **Cloud Preprocessing:** The backend validates, cleans, normalizes, and stores the data.
5. **ML Analysis:** Classification and anomaly-detection components analyze multi-parameter patterns.
6. **Risk Computation:** The system maps the analysis to the projectdefined 0–100 Laboratory Risk Score.
7. **Dashboard Update:** Risk status, trends, and contributing factors are shown to administrators.
8. **Recommendation:** The decision layer produces a recommended action based on the detected risk pattern.

### PRIVACY AND SECURITY DESIGN

The privacy objective is data minimization: access events should use pseudonymous identifiers rather than unnecessary personal names. Role-Based Access Control is proposed so that authenticated users receive only the permissions required for their roles. Secure APIs and encrypted transport are also proposed.

The security design is consistent with broader IoT guidance. NISTIR 8259A identifies device identification, data protection, logical access to interfaces, software update, cybersecurity state awareness, and device security as core IoT cybersecurity capabilities [11]. OWASP's IoT Top 10 emphasizes risks such as weak credentials, insecure network services, insecure ecosystem interfaces, insufficient privacy protection, and insecure data transfer and storage [12]. These references should be treated as design guidance; the proposed prototype does not claim formal compliance with NIST or OWASP.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

## ALERTS AND DECISION SUPPORT

The proposed alert interface has three output channels: an audible buzzer, red/yellow/green LEDs, and dashboard notifications. A SAFE state indicates normal operating conditions, WARNING indicates an anomalous condition requiring review, and CRITICAL indicates a high-risk condition requiring immediate intervention according to the project's intended operating logic.

The system is intended as decision support. A recommendation should be traceable to observed parameters and model output so that administrators can verify the underlying condition. This design is preferable to presenting an unexplained class label because it provides contextual information for human review.

## EVALUATION METHODOLOGY

The supplied project material describes the architecture and selected technologies but does not provide a completed experimental dataset, measured accuracy, precision, recall, F1-score, latency, false-alarm rate, communication overhead, or deployment energy measurements. Accordingly, this manuscript does not invent such values. A publication-grade experimental evaluation should include the following.

1. Sensor-level validation: compare sensor readings with reference instruments and report measurement error.
2. Classification evaluation: report accuracy, precision, recall, F1score, confusion matrix, and ROC-AUC where applicable.
3. Anomaly detection evaluation: report precision/recall or detection rate on labeled abnormal events, together with false-positive rate.
4. End-to-end latency: measure time from sensor observation to dashboard alert.
5. Communication evaluation: measure packet loss, transmission delay, and system behavior during temporary network interruption.
6. Privacy/security evaluation: test authentication, authorization, secure transport, pseudonymous identifiers, and common IoT attack surfaces.
7. Ablation study: compare single-parameter rules with multiparameter ML analysis to quantify the contribution of context fusion.
8. Usability evaluation: assess whether administrators can understand the risk state, contributing factors, and recommendation.

## LIMITATIONS

The present work is an architecture and prototype-oriented design. The supplied material does not establish performance using a sufficiently large real-world laboratory dataset. Sensor calibration, environmental variability, equipment diversity, model drift, network failures, and false alarms may affect practical performance. The 0–100 risk bands are project-defined design thresholds and require validation. Access monitoring also requires careful consideration of institutional privacy policies and retention requirements.

## FUTURE SCOPE

1. Build and curate a real laboratory dataset containing normal, warning, and critical operating scenarios.
2. Compare Random Forest, Decision Tree, Isolation Forest, and other suitable models using consistent evaluation protocols.
3. Add temporal features so that sustained changes and rate-of-change patterns can be analyzed.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

4. Investigate edge inference to reduce cloud dependence and communication load.
5. Add secure device provisioning, signed firmware updates, key rotation, and stronger device identity management.
6. Evaluate privacy-preserving learning or aggregation approaches for multi-laboratory deployments.
7. Develop a larger-scale dashboard with audit logs, incident history, and administrator-configurable policies.

## CONCLUSION

LabShield AI proposes a unified AIoT architecture for laboratory risk intelligence that connects multi-sensor acquisition, ESP32 edge buffering, secure communication, cloud preprocessing, machine learning, anomaly detection, explainable risk scoring, privacy-aware identification, and dashboard-based recommendations. The design responds to a practical gap between conventional sensor dashboards and integrated decision support for educational laboratories. Existing literature provides strong foundations in laboratory AIoT monitoring, predictive maintenance, IoT security, privacy protection, and cybersecurity baselines [1]–[12]. The next essential step is empirical validation using real or systematically generated laboratory scenarios. Performance claims should only be added after this evaluation is completed.

## REFERENCES

1. Qiang, S. Tang, J. Hao, L. Di Sarno, G. Wu, and M. Yin, “Integrating BIM and AIoT for Smart Engineering Laboratory Monitoring and Management,” IEEE Internet of Things Journal, vol. 12, no. 19, pp. 39844– 39861, 2025, doi: 10.1109/JIOT.2025.3587897.
2. Borghesi, A. Burrello, and A. Bartolini, “ExaMon-X: A Predictive Maintenance Framework for Automatic Monitoring in Industrial IoT Systems,” IEEE Internet of Things Journal, vol. 10, no. 4, pp. 2995–3005, 2023, doi:
3. 10.1109/JIOT.2021.3125885. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, “Securing Internet of Things Using Machine and Deep Learning Methods: A Survey,” Cluster Computing, vol. 27, pp. 9065–9089, 2024, doi:
4. 10.1007/s10586-024-04509-0.
5. Rodríguez, B. Otero, and R. Canal, “A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things,” Sensors, vol. 23, no. 3, p. 1252, 2023, doi: 10.3390/s23031252. [5] N. Alhamam, M. M. Hafizur Rahman, and A. Aljughaiman, “A Comprehensive Review on Cybersecurity of Digital Twins: Issues, Challenges, and Future Research Directions,” IEEE Access, vol. 13, pp. 45106–45124, 2025, doi: 10.1109/ACCESS.2025.3545004.
6. [6] Z. Zhang, W. Yang, F. Wu, et al., “Privacy and Integrity-Preserving Data Aggregation Scheme for Wireless Sensor Networks Digital Twins,” Journal of Cloud Computing, vol. 12, art. 140, 2023, doi: 10.1186/s13677-023-00522-7. [7] L. Breiman, “Random Forests,” Machine Learning, vol. 45, pp. 5–32, 2001, doi: 10.1023/A:1010933404324.
7. [8] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation Forest,” in Proc. IEEE International Conference on Data Mining (ICDM), 2008, pp. 413–422. [9] S. M. Lundberg and S.-I. Lee, “A Unified Approach to Interpreting Model Predictions,” in Advances in Neural Information Processing Systems 30 (NIPS 2017), 2017, pp. 4765–4774. Banks, E. Briggs, K. Borgendale, and R. Gupta, eds., “MQTT Version
8. 5.0,” OASIS Standard, Mar. 7, 2019.
9. M. Fagan, K. Megas, K. Scarfone, and M. Smith, “IoT Device Cybersecurity Capability Core Baseline,” NISTIR 8259A, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.IR.8259A.
10. OWASP Foundation, “OWASP Internet of Things Top 10,” 2018.