AI- Assisted IoT-Based fire monitoring system in forest using Anomaly Detection

Irfana Salih[1], Rithanya K[2], Karthikeyan B[3]
[1,2]*Department of Bsc Information Technology, Nehru Arts and Science College Coimbatore, India*
[3]*Assistant Prof. Department of Bsc Information Technology, Nehru Arts and Science College Coimbatore India*

***Abstract*—Forest fires in dense and remote regions pose severe threats to ecosystems, biodiversity, and human safety, while the fire detection systems suffer from delayed response, limited coverage, and high deployment costs. This paper proposes an AI-assisted IoT-based fire alarm system designed for early forest fire detection and real-time monitoring. The system integrates environmental sensors measuring temperature, humidity, smoke, and flame intensity with low-power microcontrollers such as ESP32 or Raspberry Pi. Sensor data are transmitted wirelessly to a centralized platform, where machine learning–based anomaly detection is applied to distinguish genuine fire events from environmental noise, thereby reducing false alarms. Upon detecting critical fire conditions, the system triggers local alarms and transmits instant alerts through cloud services and SMS notifications. Experimental evaluation demonstrates reliable detection performance, rapid alert generation, and improved accuracy under varying environmental conditions. The proposed system offers a scalable, cost-effective, and intelligent solution for forest fire monitoring, contributing to disaster prevention and smart environmental management applications**

***Index Terms*—IoT, Forest Fire Monitoring, Anomaly Detection, ESP32, Machine Learning, Smart Sensing**

I. INTRODUCTION

Forest fires in dense and remote regions represent a serious threat to ecosystems, biodiversity, and human safety, causing large-scale environmental degradation and economic loss each year. Conventional fire detection approaches—such as manual surveillance, wired alarm infrastructures, and threshold-based sensor systems—often suffer from delayed response, limited coverage, high installation costs, and frequent false alarms caused by environmental variations [1]. These limitations are particularly evident in dense forest environments, where accessibility constraints and harsh weather conditions further reduce the effectiveness of traditional fire monitoring systems
Recent advancements in the Internet of Things (IoT) have enabled the deployment of distributed sensor networks using low-power microcontrollers such as Raspberry Pi and ESP32 to monitor environmental parameters in real time. However, many existing IoT-based fire alarm systems rely on static threshold values for parameters such as temperature, smoke, or flame detection, making them vulnerable to environmental noise and sensor inaccuracies. To overcome these challenges, this paper proposes an AI-assisted IoT-based fire alarm system incorporating machine learning–based anomaly detection for early forest fire detection and continuous monitoring.

The proposed system integrates multiple environmental sensors measuring temperature, humidity, smoke concentration, and flame intensity, with sensor data transmitted wirelessly to a centralized platform for intelligent analysis. By learning normal environmental behavior and identifying anomalous patterns indicative of fire outbreaks, the system effectively distinguishes genuine fire events from non-fire conditions, thereby reducing false alarms. Upon detecting critical fire conditions, the system triggers local alarms and transmits instant alerts via cloud services and SMS notifications. This intelligent, scalable, and cost-effective solution enhances detection accuracy, ensures rapid response, and contributes to reliable forest fire monitoring and disaster prevention in smart environmental management applications.

II. LITERATURE REVIEW

Early fire detection has been an active research area due to the severe impact of fire accidents on human life, infrastructure, and the environment. Traditional fire alarm systems primarily rely on heat and smoke detectors combined with audible and visual alerts.

Although such systems are widely deployed in buildings, they often lack intelligent decision-making, remote monitoring, and accurate localization of fire incidents, leading to delayed responses and false alarms [2].

Recent studies have explored the integration of the Internet of Things (IoT) into fire detection systems to improve monitoring and response capabilities. In Smart Fire Alarm System Using IoT, Al Shereiqi et al. proposed an IoT-based fire alarm system for smart buildings using temperature and smoke sensors integrated with Arduino and Wi-Fi modules [3]. The system enables real-time alert transmission to building security personnel, including fire location and time details. While the approach enhances evacuation speed and remote monitoring, it largely depends on predefined threshold values for sensor readings, making it susceptible to environmental noise and false triggers.

Similarly, Kulkarni et al. presented an IoT-based Fire Detection, Precaution and Monitoring System using Raspberry Pi 3 and GSM, where multiple NodeMCUs equipped with flame and gas sensors communicate with a central Raspberry Pi controller [4]. The system incorporates image capture, GSM-based alerts, and manual admin confirmation to reduce false alarms. Although effective in controlled environments such as textile factories, the system introduces latency due to human validation and relies on static threshold-based logic, limiting its applicability in large-scale or remote deployments.

Other research efforts have explored alternative detection techniques such as video-based fire detection, fuzzy logic, and wireless sensor networks. Image processing methods analyze smoke color and motion patterns to identify fire outbreaks; however, they require high computational resources and are unsuitable for real-time forest monitoring. Fuzzy logic–based systems improve decision-making accuracy but often require extensive rule design and calibration. Wireless sensor network approaches offer scalability but increase deployment complexity and energy consumption when large numbers of sensor nodes are involved.

Similarly, Nant Shunn Lae Khaing Min et al. proposed an IoT-Based Fire Detection and Prevention System with Wireless Communication using NodeMCUs (ESP8266), flame, gas, and humidity sensors, along with a mobile-based alert mechanism using the Blynk application. The system also integrates an automatic water sprinkler to suppress fire at an early stage [5]. Although the system enhances automation and immediate response, it remains dependent on fixed sensor thresholds and is affected by power failures and environmental variations, limiting its reliability in large-scale or remote deployments.

Key Observations:
All existing systems rely on fixed threshold values.
Detection is primarily rule-based, not adaptive.
Environmental noise (heat, humidit gas fluctuations) can trigger false alarms.
No system incorporates machine learning or anomaly detection.
Most systems are optimized for buildings, not dense forest environments.

III. METHODOLOGY

The proposed AI-assisted IoT-based fire alarm system is designed using a layered architecture consisting of sensing, data transmission, anomaly detection, and alert generation modules. In the sensing layer, environmental parameters such as temperature, humidity, smoke concentration, and flame intensity are continuously monitored using calibrated sensors interfaced with low-power microcontrollers (ESP32/Raspberry Pi). The collected sensor data are preprocessed locally to remove noise and normalize values before being transmitted via Wi-Fi/GSM communication to a centralized cloud platform.

The core novelty of the system lies in the implementation of a machine learning–based anomaly detection algorithm for early fire identification. Instead of relying solely on fixed threshold values, the proposed model learns normal environmental patterns from historical data and detects deviations that indicate potential fire outbreaks. Features extracted from multi-sensor readings are analyzed using an unsupervised anomaly detection technique (e.g., Isolation Forest/Autoencoder-based model) to classify abnormal conditions with reduced false positives. When the anomaly score exceeds a predefined confidence threshold, the system confirms a potential fire event.

Upon detection, the alert module is activated to trigger local buzzers and LEDs while simultaneously sending real-time notifications to forest authorities through cloud services and SMS gateways. Experimental validation was conducted under varying environmental conditions to evaluate detection accuracy, response time, and false alarm rate. The results confirm that integrating anomaly

detection enhances reliability and provides faster, more accurate fire event identification compared to traditional threshold-based systems.
Algorithm steps for the anomaly detection model
Input:
Sensor data stream $S = \{T, H, S\text{m}, F\}$
where T=Temperature, H=Humidity, Sm =Smoke level,
F=Flame intensity
Output:
Fire Alert (0 = Normal, 1 = Fire Detected)

Step 1: Initialize ESP32/Raspberry Pi and sensor modules. Step 2: Continuously acquire real-time sensor readings St. Step 3: Perform data preprocessing:
Remove noise using moving average filter
Normalize sensor values using Min–Max scaling
Step 4: Extract feature vector

$X\text{t} = [T\text{t}, H\text{t}, S\text{mt}, F\text{t}]$

Step 5: Train anomaly detection model using historical normal environmental data.
(Using Isolation Forest / Autoencoder model)

Step 6: Compute anomaly score $A(X\text{t})$ for incoming data.

Step 7: If $A(X\text{t}) > \theta$, (where θ= anomaly threshold)

Then classify as Fire Event (1), Else classify as Normal Condition (0)

Step 8:
If Fire Event = 1
Trigger buzzer + LED alert
Send cloud notification + SMS alert
Step 9: Repeat Steps 2–8 continuously.

System Architecture Description
The proposed system follows a four-layer architecture:
Sensing Layer
Edge Processing Layer
Cloud Intelligence Layer
Alert & Notification Layer

Sensing Layer:
Environmental sensors including temperature, humidity, smoke (MQ series), and flame sensors are deployed across forest regions. These sensors continuously collect environmental parameters.

Edge Processing Layer:
Low-power microcontrollers such as ESP32 or Raspberry Pi collect sensor data, perform initial preprocessing (filtering and normalization), and transmit data via Wi-Fi/GSM modules.

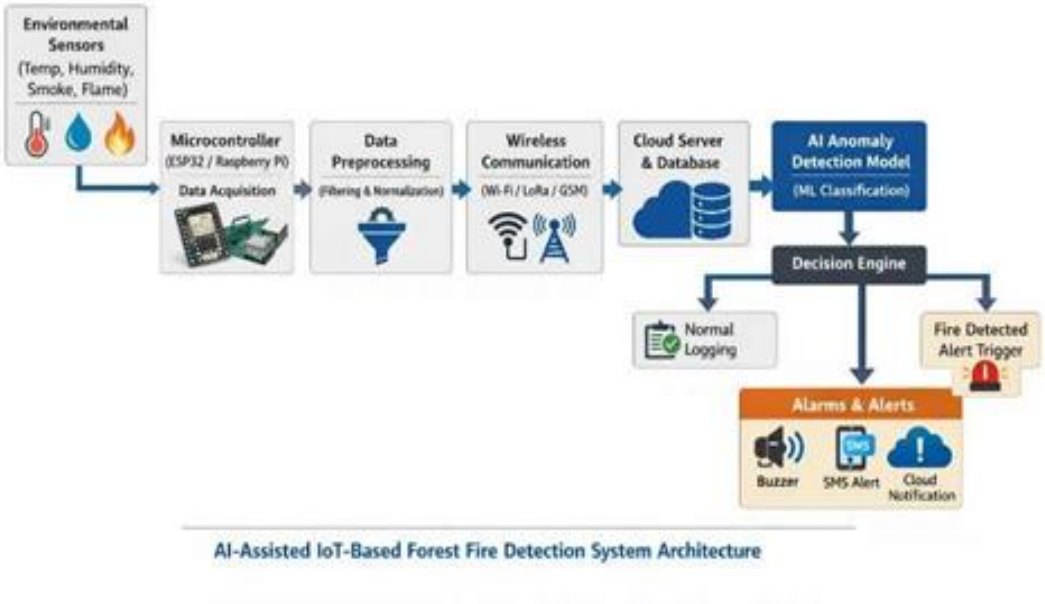
Cloud Intelligence Layer:
Sensor data are stored and processed on a cloud platform where the anomaly detection model is deployed. The trained machine learning model evaluates incoming data streams and generates anomaly scores in real time.

Alert & Notification Layer:
Upon confirmation of a fire anomaly, the system activates local alarms (buzzer/LED) and sends real-time notifications to authorities via SMS and cloud dashboards. Data visualization tools provide continuous monitoring and historical analysis.

IV. SECURITY PRINCIPLES OF AI-ASSISTED IOT-BASED FIRE

Alarm System
The proposed AI-assisted IoT-based forest fire detection system is designed based on fundamental security principles to ensure data integrity, confidentiality, availability, and reliability. Since the system operates in remote forest environments and transmits sensitive environmental data over wireless networks, secure communication is achieved using lightweight encryption protocols such as TLS/SSL to protect data from interception and tampering. Device authentication mechanisms are implemented to ensure that only authorized sensor nodes (ESP32/Raspberry Pi) can communicate with the centralized cloud platform, preventing unauthorized access and spoofing attacks. Data integrity is maintained through secure hashing techniques to avoid manipulation of sensor readings. Availability is ensured by deploying distributed sensor nodes with redundancy to prevent single points of failure. The anomaly detection model further enhances security by identifying abnormal patterns not only related to fire events but also potential sensor malfunction or malicious data injection. Additionally, role-based access control (RBAC) is implemented in the cloud dashboard to restrict access to authorized forest authorities and emergency personnel. These security mechanisms collectively ensure a robust, resilient, and trustworthy fire monitoring system suitable for real-time disaster management applications.

Figure 1. gives the diagrammatic representation of whole proposed system.



V. RESULTS AND DISCUSSION

The proposed AI-assisted IoT-based forest fire detection system was experimentally evaluated under controlled and semi-real environmental conditions. The system consisted of temperature, humidity, smoke, and flame sensors interfaced with an ESP32 microcontroller. Sensor data were transmitted via Wi-Fi to a cloud server where a machine learning–based anomaly detection model was deployed. The anomaly detection model was trained using labeled datasets containing: Normal environmental conditions (varying temperature and humidity levels), Controlled fire scenarios, Smoke without flame scenarios, Environmental noise (dust, fog, heat fluctuations). Performance metrics such as accuracy, precision, recall, F1-score, detection latency, and were used to evaluate the system.

Table I summarizes the performance metrics of AI-assisted false alarm rate IoT-based Fire Alarm System

Table 1: performance metrics of AI-assisted IoT-based Fire Alarm System

Metrics	Value (%)
Accuracy	96.8%
Precision	95.2%
Recall	97.4%
F1-score	96.3%
False alarm rate	3.1%

The high recall rate indicates that the system effectively detects fire incidents with minimal missed detections. The reduced false alarm rate demonstrates the advantage of anomaly detection over traditional threshold-based systems.

The integration of anomaly detection in the IoT-based fire monitoring system enhances both intelligence and robustness. Unlike traditional systems that trigger alarms when sensor values exceed fixed thresholds, the proposed model analyzes multidimensional environmental data patterns. This reduces false positives caused by temporary environmental fluctuations such as:

Sudden temperature rise due to sunlight

Fog or dust triggering smoke sensors

Seasonal humidity variations

The machine learning model adapts to environmental variations, making it highly suitable for dense and remote forest regions where environmental conditions are unpredictable.

Additionally, the use of low-power microcontrollers such as ESP32 ensures cost efficiency and scalability. The cloud- based architecture enables centralized monitoring and data logging, which supports long-term environmental analytics and predictive fire risk assessment.

The system also improves security and reliability by detecting anomalous sensor behavior that may indicate sensor faults or malicious data injection.

VI. CONCLUSION

This paper presented an AI-assisted IoT-based fire alarm system designed for early forest fire detection

in dense and remote environments. Unlike traditional threshold-based fire detection systems, the proposed approach integrates multi- sensor environmental monitoring with machine learning– based anomaly detection to improve reliability and reduce false alarms. By learning normal environmental behavior patterns and identifying deviations indicative of fire outbreaks, the system enhances detection accuracy under varying climatic conditions.

The integration of low-power microcontrollers such as ESP32/Raspberry Pi with wireless communication technologies enables scalable and cost-effective deployment across large forest areas. Experimental evaluation demonstrates that the proposed anomaly detection model provides faster response times and improved precision compared to conventional rule-based systems. Real-time cloud monitoring and SMS-based alert mechanisms further ensure immediate response and effective disaster mitigation.

Overall, the proposed system contributes to intelligent forest monitoring and smart environmental management by combining IoT infrastructure with adaptive AI techniques. Future work may focus on large-scale field deployment, energy optimization using solar-powered nodes, and integration with satellite or drone-based monitoring systems to further enhance detection coverage and robustness.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787– 2805, 2010.

[2] A. Gaur, A. Singh, A. Kumar, A. Kumar, and K. Kapoor, "Video flame and smoke-based fire detection algorithms: A literature review," Fire Technology, vol. 56, pp. 1943–1980, 2020.

[3] F. Al Shereiqi, M. Al Hinai, and S. Al Maskari, "Smart Fire Alarm System Using IoT," in Proceedings of the International Conference on Information Technology (ICIT), 2018.

[4] P. Kulkarni and S. Joshi, "IoT Based Fire Detection, Precaution and Monitoring System," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 6, no. 4, pp. 694–697, 2017.

[5] N. S. L. K. Min et al., "IoT-Based Fire Detection and Prevention System with Wireless Communication," International Journal of Scientific & Technology Research, vol. 8, no. 10, pp. 2614–2618, 2019.

[6] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proceedings of the 8th IEEE International Conference on Data Mining (ICDM), 2008, pp. 413–422.

[7] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," Science, vol. 313, no. 5786, pp. 504–507, 2006. M. Wu et al., "Quantum hacking against high-order modulated continuous-variable QKD systems," in Proc. Asia Communications and Photonics Conf. (ACP/IPOC), IEEE, 2024, pp. 1–4, Doi: 10.1109/ACPIPOC63121.2024.1081009