



Cloud-Integrated Iot System For Health Monitoring With Automated Gate Access Control

Cheerla Pooja Rani, Dasari Neha Sree, Gundapu Venkata Lokesh Karunakar, Galla Bhavani, Busam Hemanth

Assistant professor, UG, UG, UG, UG
Dept of Information Technology,

Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India

Abstract: Traditional access control systems primarily verify identity but lack real-time health monitoring, which is crucial in high-risk environments such as campuses, laboratories, hospitals, and industries. This project presents a Cloud-Integrated IoT Secure Entry System that ensures automated, secure, and health-compliant access. The system integrates fingerprint authentication, mask detection (using OpenCV & CNN), temperature sensing (MLX90614), and alcohol detection (MQ-3) to assess an individual's health status before granting access. If all safety conditions are met, a servo motor-controlled gate allows entry, ensuring a contactless and automated process. The system utilizes Node MCU ESP8266 for IoT implementation, enabling real-time cloud storage, monitoring, and automated reporting to enhance security and compliance while reducing manual intervention. Testing results demonstrate high accuracy in biometric authentication and health parameter detection, ensuring reliable access control. The cloud integration allows remote monitoring and quick response to security breaches or health risks. The system significantly enhances safety and operational efficiency in restricted areas. This IoT-based solution bridges the gap between security and health compliance, offering an innovative approach to automated access control. Future improvements may include AI-driven risk assessment and broader sensor integration for enhanced monitoring.

Keywords: IoT, Secure Entry System, Access Control, Health Compliance, Fingerprint Authentication, Mask Detection, OpenCV, CNN, Temperature Sensing, MLX90614, Alcohol Detection

I. INTRODUCTION

Access control systems play a crucial role in ensuring security and regulating entry in various environments such as campuses, laboratories, hospitals, and industries. Traditional access control methods primarily focus on identity verification through ID cards, PIN codes, or biometric authentication, such as fingerprint or facial recognition. However, these methods fail to incorporate real-time health monitoring, which is essential in high-risk environments where individuals' health conditions could pose security threats. The COVID-19 pandemic highlighted the significance of health-compliant access control systems, emphasizing the need for mask detection, temperature screening, and alcohol detection. A system that integrates security and health compliance can significantly reduce risks associated with the spread of infectious diseases and workplace safety hazards.

The Cloud-Integrated IoT Secure Entry System presented in this project is designed to enhance traditional access control by integrating health-monitoring features. The system employs fingerprint authentication for identity verification, mask detection using OpenCV and Convolutional Neural Networks (CNNs), temperature sensing via MLX90614 infrared sensor, and alcohol detection using the MQ-3 sensor. Access is granted only when all safety conditions are met, ensuring that individuals who exhibit signs of illness or intoxication are

denied entry. A servo motor-controlled gate automates the entry process, making it completely contactless, which is particularly beneficial in reducing the spread of infectious diseases. The integration of multiple sensors and AI-based detection mechanisms ensures a high level of accuracy and reliability in the system's decision-making process.

The system is powered by the NodeMCU ESP8266 microcontroller, which enables IoT connectivity, allowing real-time data storage, monitoring, and automated reporting through cloud integration. This feature significantly enhances security and operational efficiency by providing remote access control, instant alerts for policy violations, and detailed reports for compliance tracking. Additionally, cloud-based monitoring allows administrators to oversee multiple entry points from a centralized dashboard, reducing the need for manual intervention. The use of IoT in security applications not only improves response time but also facilitates data-driven decision-making, leading to more effective enforcement of health and safety protocols.

By integrating biometric authentication, AI-powered health monitoring, and IoT-based cloud connectivity, this system bridges the gap between traditional access control and modern health safety requirements. The implementation of real-time monitoring and automated reporting reduces human effort while increasing security and efficiency. The proposed system is particularly useful in settings where maintaining strict health and safety regulations is critical, such as hospitals, research labs, and manufacturing units dealing with hazardous materials. Future enhancements may include AI-driven predictive analytics to assess risk levels, integration with government health databases for real-time updates, and expansion to smart city infrastructures for broader security applications. This project demonstrates a scalable, intelligent, and health-compliant security solution, paving the way for smarter and safer access control systems in the future.

1.2 Motivation:

Traditional access control systems focus solely on identity verification, neglecting critical health parameters that can impact safety in high-risk environments. The COVID-19 pandemic emphasized the need for health-compliant security measures to prevent disease transmission. Additionally, workplaces such as laboratories, hospitals, and industries face risks from intoxicated or unwell individuals, leading to potential hazards. This project aims to integrate biometric authentication, mask detection, temperature sensing, and alcohol detection into a cloud-connected IoT system for secure, automated access. By reducing manual intervention and enhancing real-time monitoring, the system ensures efficient, contactless, and health-compliant entry, improving overall security and operational efficiency.

1.3 Objectives:

- Develop an IoT-based automated access system that integrates biometric authentication and health monitoring for secure entry.
- Verify identity and health compliance in real-time using fingerprint authentication, mask detection, temperature sensing, and alcohol detection.
- Implement real-time monitoring with NodeMCU and cloud storage to enable remote access control, data logging, and automated reporting.
- Ensure safety in workplaces, laboratories, and industrial areas by providing a contactless authentication system that minimizes manual intervention and enhances security compliance.

1.4 Literature Survey:

Zhang et al. introduced a location-based access control mechanism for cloud-stored data, focusing on policy hiding and privacy preservation[1]. The proposed framework ensures that access policies remain hidden from cloud service providers while still enforcing fine-grained access control. By utilizing fully outsourced encryption and decryption, their approach enhances security while reducing computational overhead for end-users. This work is significant in cloud security as it prevents unauthorized access while maintaining data confidentiality. However, its primary focus is on data access control rather than physical entry systems, making it less applicable to real-time access control scenarios in IoT-based security frameworks.

Bhattacharya et al. expanded on secure access control mechanisms by introducing BinDaaS for industrial IoT security and privacy. Their model leverages blockchain technology to ensure tamper-proof access control and data integrity in IoT environments[2]. The decentralized nature of blockchain eliminates single points of failure, making it a robust alternative to traditional cloud-based authentication models. While this work significantly enhances security in IoT-driven environments, it does not specifically address health-compliant access control, which is crucial in high-risk areas like hospitals and laboratories. Integrating blockchain with biometric and health-monitoring mechanisms could further improve security in automated IoT-based entry

systems.

Kadhim et al. proposed a smart access control system leveraging IoT and cloud computing to enhance security and efficiency in restricted environments. Their system integrates biometric authentication and real-time monitoring, ensuring secure access while enabling remote management through cloud infrastructure[3]. By utilizing NodeMCU ESP8266 for IoT implementation, the model facilitates automated decision-making and centralized control, reducing manual intervention. However, while the system provides secure identity verification, it lacks comprehensive health monitoring features such as mask detection, temperature sensing, and alcohol detection, which are crucial for access control in health-sensitive environments like hospitals and laboratories.

Kakkavas et al. introduced a zero-trust access control model that incorporates blockchain and AI-based authentication to strengthen security in cloud and IoT ecosystems. Their approach eliminates implicit trust by continuously verifying user identity and assessing risk factors before granting access[4]. The use of blockchain technology ensures tamper-proof logging, preventing unauthorized modifications to access control records. While this model enhances cybersecurity and privacy, it does not specifically address physical entry barriers or real-time health assessments. Integrating AI-driven biometric authentication with health compliance checks could further improve access control systems, particularly in high-risk environments requiring strict health regulations.

1.5 CNNs Model

Convolutional Neural Networks are a class of deep learning models specifically designed for image processing tasks such as object detection, facial recognition, and health compliance monitoring. Unlike traditional feedforward neural networks, CNNs utilize convolutional layers to extract spatial features from images, making them highly effective for visual pattern recognition. TensorFlow, an open-source deep learning framework, provides powerful tools for implementing CNNs efficiently, while OpenCV facilitates real-time image processing. A standard CNN consists of multiple layers, including convolutional layers, activation functions, pooling layers, fully connected layers, and softmax classification. The convolutional operation is defined as:

$$Z_{i,j} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} X_{i+m,j+n} \cdot K_{m,n} + B$$

where X is the input image, K is the convolutional filter (kernel), B is the bias term, and Z is the output feature map. TensorFlow allows CNNs to be implemented efficiently using the tf.keras module. A typical CNN model for mask detection or face recognition in TensorFlow is constructed with Conv2D layers for feature extraction, MaxPooling2D for dimensionality reduction, and Dense layers for classification. OpenCV (cv2) is used for real-time image preprocessing, including grayscale conversion, Gaussian blurring, and edge detection. The pooling operation, used to reduce feature map size, is defined as:

$$P_{i,j} = \max(Z_{2i,2j}, Z_{2i+1,2j}, Z_{2i,2j+1}, Z_{2i+1,2j+1})$$

where Max Pooling selects the highest pixel value in a local region to retain the most significant features. CNNs implemented using TensorFlow and OpenCV offer a highly scalable solution for tasks such as mask detection, facial recognition, and security authentication.

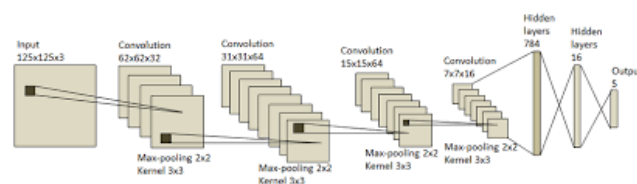


Fig1:CNN model

By integrating these models into IoT-based access control systems, real-time health compliance monitoring can be achieved, ensuring secure, automated, and health-conscious entry control in restricted environments.

1.6 Components Used

1.6.1 ESP8266 WiFi Module

The ESP8266 WiFi module is a low-cost, high-performance microcontroller used to enable IoT-based communication by connecting sensors to the cloud. It facilitates real-time data transmission by interfacing with various components such as temperature sensors, fingerprint readers, and gas sensors.



Fig2:ESP8266 Module

Using protocols like MQTT and HTTP, ESP8266 sends data to cloud platforms such as Firebase, AWS, or Thingspeak, allowing for remote monitoring and automated alerts. In a secure entry system, the ESP8266 ensures seamless cloud integration, enabling centralized data storage and analysis for improved security, compliance, and automation.

1.6.2 MQ-3 Gas Sensor

The MQ-3 gas sensor is a widely used module for alcohol detection in breath analysis applications. It operates by detecting ethanol vapors in a person's breath and producing an analog voltage output corresponding to the alcohol concentration.

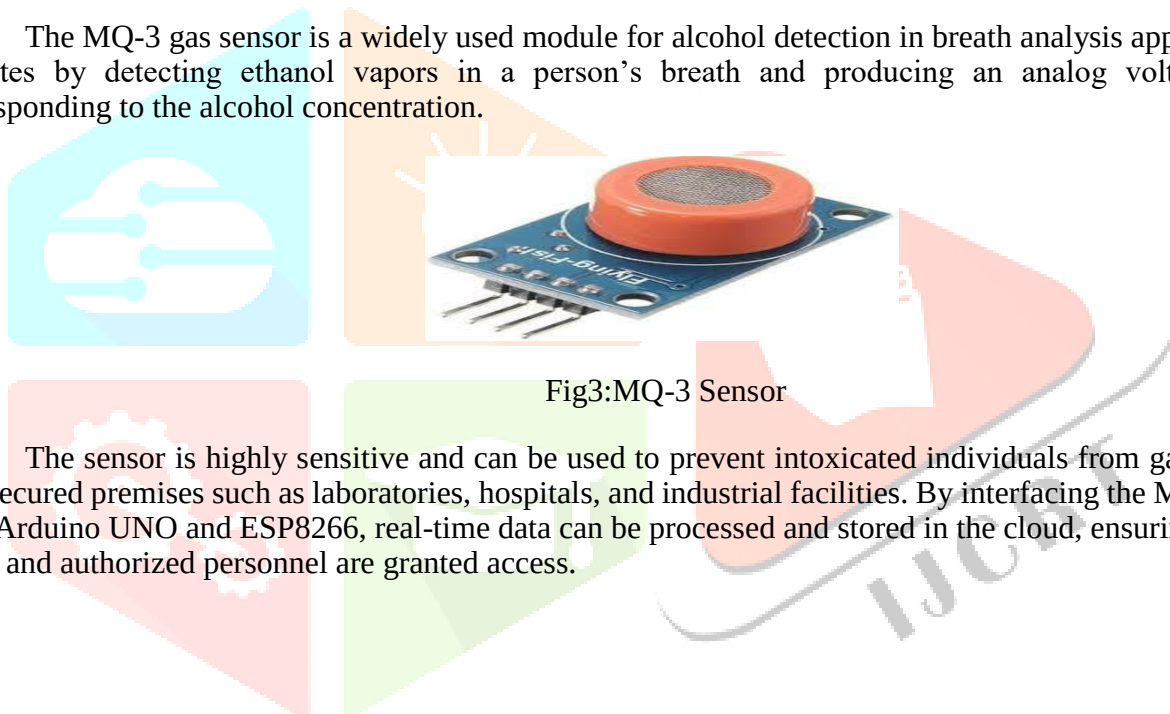


Fig3:MQ-3 Sensor

The sensor is highly sensitive and can be used to prevent intoxicated individuals from gaining entry into secured premises such as laboratories, hospitals, and industrial facilities. By interfacing the MQ-3 sensor with Arduino UNO and ESP8266, real-time data can be processed and stored in the cloud, ensuring that only sober and authorized personnel are granted access.

1.6.3 MLX90614

The MLX90614 infrared temperature sensor is a non-contact thermometer used for fever detection in security and health-compliant access control systems.



Fig4:Temperature sensor

It measures body temperature by detecting infrared radiation emitted from a person's skin and provides an accurate digital output. This feature is crucial in preventing individuals with high body temperatures (potential fever symptoms) from entering restricted areas. The MLX90614 integrates with ESP8266 and sends real-time temperature readings to the cloud, ensuring automated health screening and compliance with safety

regulations in hospitals, research labs, and industrial zones.

1.6.4 Servo Motor and Fingerprint Reader

A servo motor is used to control the automated gate mechanism, allowing entry only if all security conditions are met. The motor receives signals from the microcontroller (Arduino or ESP8266), which processes sensor data from fingerprint scanners, alcohol detectors, and temperature sensors.

A fingerprint reader enhances biometric security by scanning and verifying an individual's fingerprint before granting access. The scanner captures the fingerprint's unique ridge patterns, converts them into a digital format, and matches them with stored templates in the database.

1.6.5 ESP32-CAM

The ESP32-CAM is a low-power AI-enabled camera module used for facial recognition-based access control. It captures an image of the user and processes it using machine learning models for identity verification.

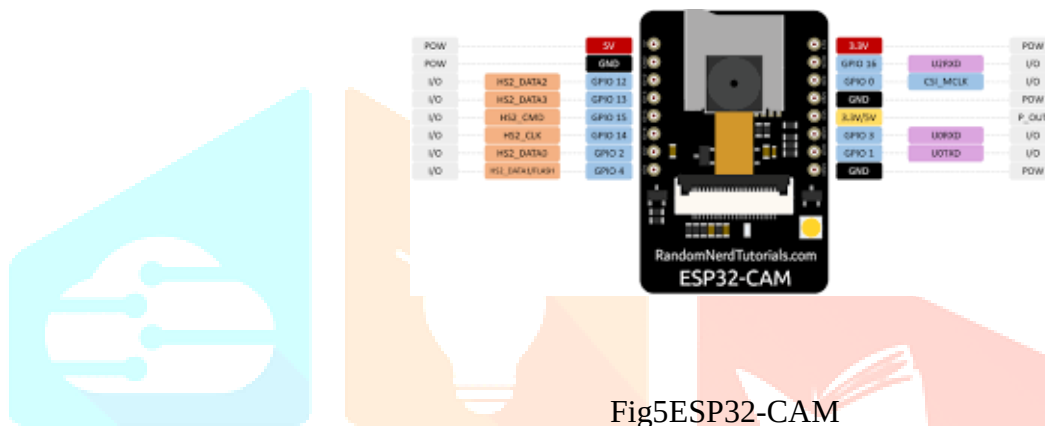


Fig5ESP32-CAM

Integrated with TensorFlow Lite, OpenCV, and cloud databases, the ESP32-CAM allows real-time facial authentication, enhancing contactless security solutions. When combined with mask detection algorithms, the system ensures that only individuals wearing a face mask and matching the authorized database are allowed entry. This module plays a crucial role in AI-driven access control, reducing manual verification efforts while improving safety and efficiency.

1.6.6 Arduino UNO

The Arduino UNO serves as the central microcontroller that integrates all sensors and components in the secure entry system. It processes input data from the MQ-3 gas sensor, MLX90614 temperature sensor, fingerprint reader, and ESP32-CAM, sending processed information to the ESP8266 for cloud communication. The Arduino's digital and analog pins facilitate seamless interfacing with servo motors, biometric scanners, and security modules, ensuring smooth operation.



Fig 6:Arduino UNO

As an open-source microcontroller, the Arduino UNO provides a cost-effective and customizable solution for implementing automated, health-compliant access control systems in campuses, hospitals, and industries.

II. PROPOSAL METHOD

The proposed Cloud-Integrated IoT Secure Entry System enhances security by integrating biometric authentication (fingerprint scanning) with real-time health monitoring, ensuring that only authorized and health-compliant individuals gain entry. By incorporating mask detection using OpenCV and CNN, temperature screening with MLX90614, and alcohol detection via the MQ-3 sensor, the system prevents entry to individuals who are sick, intoxicated, or non-compliant with safety measures.

The system's automated access mechanism is controlled by a servo motor, which operates the entry gate only when all security and health conditions are met. A NodeMCU ESP8266 WiFi module ensures real-time data transmission to the cloud, enabling remote monitoring, automated alerts, and compliance tracking. The ESP32-CAM module further strengthens security by capturing facial images for mask detection and identity verification. This seamless IoT-based approach eliminates the need for manual intervention, reducing operational inefficiencies while maintaining strict access control in sensitive areas.

Biometric security plays a crucial role in ensuring secure access control by uniquely identifying individuals. In this system, a fingerprint authentication module is used as the primary identity verification mechanism. Each user's fingerprint is scanned, converted into a digital template, and matched against a pre-stored database. If the scanned fingerprint is valid, the individual is granted access; otherwise, entry is denied. Unlike traditional access cards or PIN-based systems, fingerprint authentication eliminates security loopholes such as card theft or password sharing. Integrated with Arduino UNO and ESP8266, the fingerprint module provides real-time verification, ensuring that only authorized personnel can enter restricted areas such as research labs, hospitals, and corporate offices.

In environments where health compliance is essential, mask detection is integrated into the system using OpenCV and a Convolutional Neural Network (CNN). The ESP32-CAM captures an image of the person attempting to gain entry, and OpenCV processes the image for pre-processing operations like grayscale conversion and feature extraction. A trained CNN model then classifies whether the person is wearing a mask or not. If a mask is detected, the system proceeds to the next authentication step. Otherwise, access is denied. This contactless method ensures compliance with health safety regulations, especially in settings such as hospitals, pharmaceutical industries, and public facilities, where controlling infection spread is crucial.

Fever is one of the primary symptoms of infections, making temperature screening an essential step in health-sensitive access control systems. The MLX90614 infrared temperature sensor is integrated into the system to measure body temperature without physical contact. When an individual approaches the entry point, the sensor detects their forehead temperature and transmits the data to the microcontroller (Arduino/ESP8266). If the temperature is within the normal range ($\leq 37.5^{\circ}\text{C}$), the person proceeds to the next verification stage. However, if the temperature is above the threshold, the system automatically denies access and sends an alert notification to the cloud for health monitoring authorities. This step ensures that individuals with potential fever symptoms are restricted from entering high-risk areas.

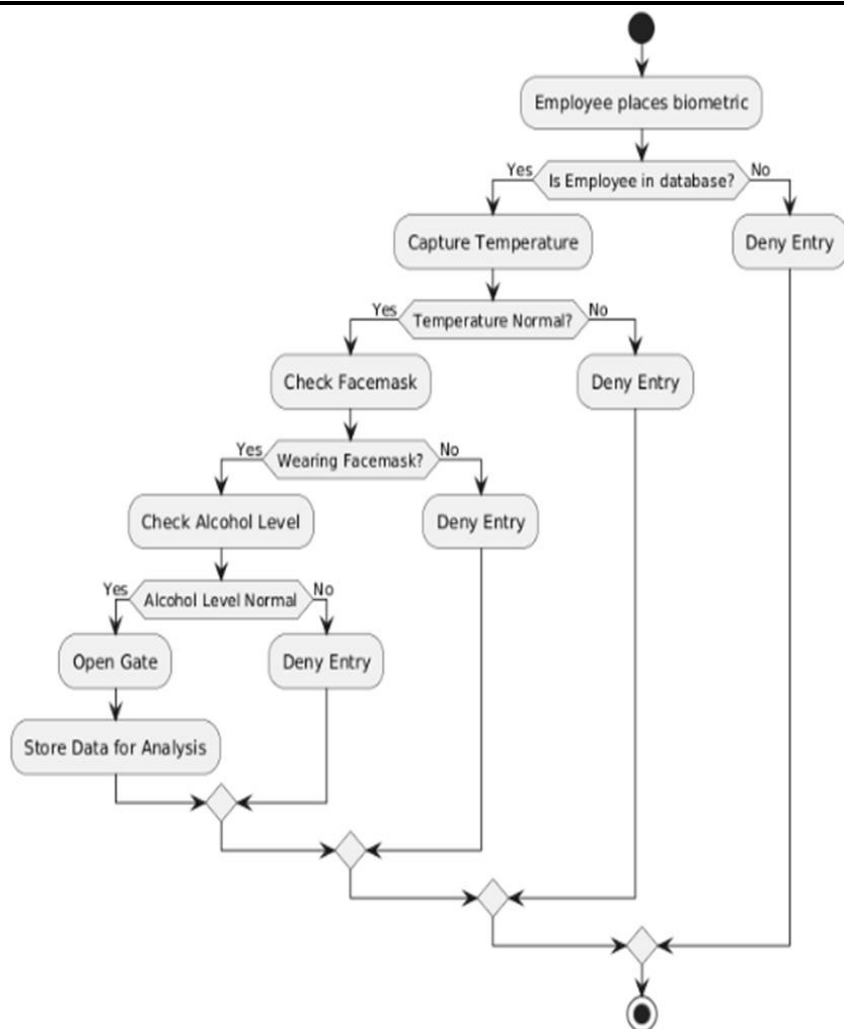


Fig7:Proposal Diagram

The MQ-3 alcohol sensor is implemented to detect alcohol intoxication in individuals attempting to gain access. This is particularly important for industries, laboratories, and workplaces where precision and alertness are critical. The MQ-3 sensor measures ethanol concentration in the breath and generates an analog output proportional to the alcohol level detected. If the alcohol level exceeds a predefined threshold, access is immediately denied, and a security alert is triggered. By preventing intoxicated individuals from entering, the system enhances workplace safety, reduces accident risks, and ensures compliance with occupational safety regulations.

Once all authentication and safety checks are successfully passed, an automated gate mechanism is activated using a servo motor. The servo motor is controlled by the Arduino UNO or ESP8266, which processes sensor inputs and generates a PWM signal to rotate the servo arm. If all conditions are met, the servo motor unlocks and opens the gate. Otherwise, the gate remains locked. This mechanism eliminates manual intervention, ensuring a fully automated, touchless, and secure access system. The servo motor-driven gate is ideal for smart buildings, hospitals, and high-security zones, where quick and efficient entry management is required.

To enhance remote monitoring and centralized control, the ESP8266 WiFi module is used to connect the system to the cloud. Sensor data, including biometric records, temperature readings, alcohol detection levels, and entry logs, is stored on cloud platforms such as Firebase, AWS, or Thingspeak. This enables real-time data access, allowing security administrators to monitor entry activities remotely. Additionally, automated reports can be generated for compliance auditing, ensuring that only authorized and health-compliant individuals gain entry. The ESP8266's cloud connectivity also allows for instant notifications in case of security breaches or health violations, making the system highly efficient, scalable, and future-ready for IoT-based smart security solutions.

III. Hardware and Software Requirements

The Cloud-Integrated IoT Secure Entry System requires both hardware and software components to ensure seamless operation. The hardware components include a NodeMCU ESP8266 WiFi module for IoT connectivity and cloud communication, an Arduino UNO microcontroller for sensor integration and processing, a fingerprint scanner for biometric authentication, an ESP32-CAM module for facial recognition and mask detection, an MLX90614 infrared temperature sensor for fever screening, an MQ-3 alcohol sensor for detecting intoxication, and a servo motor for automated gate control. Additional components such as relays, jumper wires, power supply units, and a display (LCD or OLED) may be used for real-time feedback. The software requirements include Arduino IDE for programming the microcontrollers, Python with OpenCV and TensorFlow for image processing and machine learning-based mask detection, and cloud platforms like Firebase, AWS, or Thingspeak for data storage and real-time monitoring. The MQTT or HTTP protocol is used for secure cloud communication, and database management systems handle access logs and authentication records. This integration of hardware and software ensures an automated, intelligent, and health-compliant access control system, suitable for deployment in hospitals, industries, laboratories, and corporate offices.

IV. RESULTS

The Dashboard provides a detailed track history and report of employee health compliance, offering real-time insights into access control violations. It allows administrators to filter data based on Employee ID, date range, and specific conditions, ensuring efficient monitoring of workplace safety. The system logs events such as alcohol detection, fever symptoms, and mask violations, enhancing accountability and security. The visual representation of historical data aids in trend analysis, helping organizations enforce health policies effectively. By generating automated reports, the dashboard ensures compliance tracking, supporting a safer and more controlled work environment.

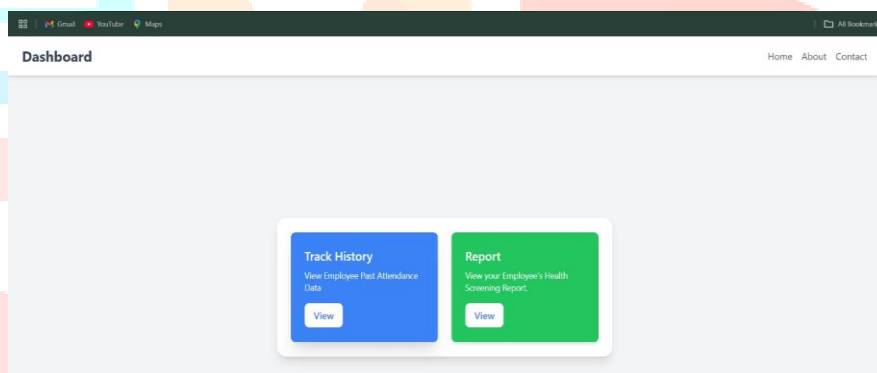


Fig 8: Dashboard

The Attendance History module logs employee access events, providing a clear record of entry and exit times. By integrating biometric authentication and IoT-based monitoring, the system ensures accurate tracking of attendance without manual intervention. Administrators can retrieve attendance data based on employee ID and date filters, enabling workforce management and productivity analysis. This data can be used for payroll processing, shift management, and performance evaluation.

Employee ID	Employee Name	Date	Status
E161	Suraj	2025-03-07 13:31:51	Not Attended
E131	vijay	2025-02-28 14:24:56	Not Attended
E131	vijay	2025-02-12 16:21:05	Attended
E134	srinanth	2025-02-10 16:21:21	Not Attended
E143	saravith	2025-02-07 16:22:10	Not Attended
E123	Hemant	2025-02-04 16:13:11	Attended
E145	haril	2025-02-03 16:22:30	Not Attended

Fig 9: Attendance History

Additionally, attendance history helps in identifying anomalies, such as unauthorized access attempts or irregular attendance patterns, making the system a reliable solution for workplace security and efficiency.

The Employee Health Monitoring system provides a comprehensive record of health-related access restrictions, ensuring a safe and compliant workplace. The system tracks health conditions, such as alcohol detection, fever symptoms, and mask violations, preventing non-compliant employees from entering restricted areas. Administrators can review logs by employee ID, date, and specific health conditions, allowing for proactive intervention and workplace safety improvements. This system supports regulatory compliance, minimizes health risks, and enhances workplace hygiene standards. By maintaining detailed records, organizations can implement preventive measures, ensuring a secure and health-conscious working environment.

Employee Health Monitoring

Enter Employee
E145

From
01-02-2025

To
01-03-2025

Condition
All

Filter

Employee ID	Date	Condition Status
E145	Sat, 01 Mar 2025 14:28:23 GMT	Alcohol Detected
E145	Mon, 03 Feb 2025 16:22:20 GMT	No Mask

Health Condition Overview

Fig 10:Health Monitoring

V. CONCLUSION:

In conclusion, the Cloud-Integrated IoT Secure Entry System successfully enhances access control and workplace safety by integrating biometric authentication, real-time health monitoring, and cloud-based data storage. By combining fingerprint recognition, mask detection using OpenCV and CNN, temperature screening with MLX90614, and alcohol detection via the MQ-3 sensor, the system ensures that only authorized and health-compliant individuals gain entry. The automated access mechanism, controlled by a servo motor, eliminates manual intervention, improving efficiency and security in high-risk environments like hospitals, industries, and research facilities. With real-time monitoring and cloud connectivity via NodeMCU ESP8266, organizations can track employee health conditions, generate reports, and enhance policy enforcement, ensuring a safer and smarter workplace.

VI. FUTURE WORK:

For future work, the system can be enhanced with AI-driven anomaly detection to identify unusual access patterns and potential security threats. Integration with facial recognition can further strengthen authentication, reducing reliance on physical biometrics. The system can also support multi-factor authentication (MFA) for higher security levels. Expanding cloud-based analytics will allow for predictive monitoring, enabling organizations to implement preventive measures before health risks escalate. Additionally, extending compatibility with IoT-enabled wearables can provide continuous health tracking, making access control even more dynamic and responsive.

VII.References:

- 1.Zhang Y, Chen X, Li J, Wong D, Lee P, Lou W. Ensuring location-based access control for cloud-stored data with fully outsourced policy hiding. *IEEE Transactions on Information Forensics and Security*. 2016;11(8): 1941-1955.
- 2.Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. BinDaaS: Blockchain-integrated data-as-a-service for industrial IoT security and privacy. *Future Generation Computer Systems*. 2020;101: 1020-1037.
- 3.Kadhim A, Alsahag M, Obeidat A, Jamel N, Alrubian S. Smart access control system based on IoT and cloud computing. *IEEE Access*. 2022;10: 10201-10215.
- 3.Kakkavas G, Katos V, Karantias S. A zero-trust access control model using blockchain and AI-based authentication. *Computers & Security*. 2023;130: 103354.
- 4.Mehmood Y, Ahmad F, Afzal M, Anwar M. Internet-of-Things-based smart cities: Recent advances and challenges. *IEEE Communications Surveys & Tutorials*. 2017;19(3): 2456-2476.
- 5.Narmadha P, Sindhu M. IoT-enabled intelligent biometric access control system with real-time

monitoring. *Wireless Personal Communications*. 2021;118(3): 2029-2052.

6.Chatterjee S, Nath S. Secure cloud-based health monitoring system using IoT and artificial intelligence. *International Journal of Information Management*. 2021;58: 102298.

7.Kumar S, Sharma P, Bera R. Smart access control using facial recognition and deep learning. *Multimedia Tools and Applications*. 2022;81: 18167-18190.

8.Barik R, Hota H, Singh D. A deep learning-based smart surveillance system for healthcare access control. *Expert Systems with Applications*. 2022;187: 115883.

9.Rahman A, Islam S, Kim J, Hong C. Secure IoT-based smart healthcare framework for real-time monitoring. *Journal of Network and Computer Applications*. 2019;137: 23-35.

10.Sharma V, Chen M, Moon S. IoT-based security framework for cloud-integrated access control systems. *IEEE Transactions on Cloud Computing*. 2022;10(1): 189-202.

11.Tanwar S, Tyagi S, Kumar N. The role of machine learning in IoT-based smart access control systems. *Journal of Ambient Intelligence and Humanized Computing*. 2020;11: 1465-1485.

12.Sun L, Tian H, Yu H. Blockchain-based decentralized authentication for cloud-enabled IoT. *Future Generation Computer Systems*. 2021;115: 767-778.

13.Singh A, Kumar R. An intelligent IoT-based health monitoring system using AI. *Sustainable Cities and Society*. 2021;74: 103189.

14.Pandey S, Litoriya R. Role of deep learning in security applications for smart environments. *IEEE Access*. 2021;9: 118562-118582.

15.Zhang Z, Li H, Ma Z, Liu C. Secure IoT-based cloud authentication model using federated learning. *Neurocomputing*. 2022;488: 152-166.

16.Alsaadi A, Hina R, Rahman A. Real-time IoT-based biometric authentication for secure access control. *Journal of Supercomputing*. 2022;78: 4986-5009.

17.Verma A, Sood S, Kumar N. A cloud-integrated smart authentication framework for secure IoT-based applications. *Journal of Cloud Computing*. 2021;10(1): 1-17.

18.Abu M, Chien H, Leu F. A secure facial recognition-based access control system for IoT. *Future Internet*. 2020;12(6): 101.

19.Mohamed A, Wahab F, Elhoseny M. IoT-enabled cloud-based smart security access system using deep learning. *IEEE Access*. 2022;10: 18071-18085.

