***Internet of Everything***

***Continuous Assessment - 1***

**Name: Shashwat Tripathi**

**Division: D20A**

**Roll no: 64**

**1. Identify and list all the computational activities and Scope of the application**

**Real-time Environmental Monitoring**: Continuous tracking of smoke, gas levels, and flame presence in industrial environments.

**Response to Emergencies**: Immediate alerts and automated response to potential hazards (e.g., dangerous gas levels, detected flames, or excessive smoke).

**Safety Compliance Management**: Monitoring and ensuring adherence to safety regulations. Automated reporting for regulatory compliance.

**Environmental Data Storage and Analysis**: Long-term storage of environmental metrics and incident records on the cloud. Advanced analytics to provide insights into safety trends and potential risk factors.

**Security and Compliance**: Ensuring data privacy and compliance with industrial safety standards. Secured data transmission and storage.

**Scalability and Integration**: Ability to integrate with other IoT devices, industrial systems, or safety platforms.

**User Interface and Experience**: Display real-time data and visual reports through intuitive interfaces. Easy access to historical data and safety records.

**User Notifications and Alerts**: Generate and send alerts for potential hazards and safety breaches. Notifications for maintenance checks and system updates.

**2. Segregate the various computational activities at various layers - Edge, FOG and Cloud**

| **Functionality** | **Edge Layer** | **Fog Layer** | **Cloud Layer** |
| --- | --- | --- | --- |
| **Real-time Hazard Detection** | Action: Monitor smoke, gas levels, and flame presence using **smoke sensors, gas sensors, and flame detectors**.  Response: Trigger immediate alerts on detection of hazards. | Action: Aggregate data from multiple sensors for enhanced detection accuracy.  Response: Filter and analyze data trends. | Action: Store historical detection data and analyze it for long-term trends.  Response: Generate reports for compliance and audits. |
| **Alert Generation and Notification** | Action: Generate alerts on-site (e.g., sirens, flashing lights) when hazards are detected.  Response: Notify personnel immediately. | - | - |
| **User Interface and Monitoring** | Action: Display real-time data and alerts on a local user interface.  Response: Provide a visual dashboard for on-site personnel. | Action: Aggregate and summarize data for display on broader monitoring systems.  Response: Create a centralized interface for operators. | Action: Provide a web-based dashboard for remote monitoring.  Response: Enable users to view historical data and alerts from anywhere. |
| **Data Logging and Reporting** | Action: Log detection events locally for immediate access.  Response: Maintain records of all detection incidents. | Action: Compile logs from multiple sensors for a comprehensive view of incidents.  Response: Prepare data for cloud backup. | Action: Store long-term logs and generate reports for regulatory compliance.  Response: Facilitate audit trails and trend analysis. |
| **Maintenance and Calibration** | Action: Monitor sensor performance and trigger alerts for maintenance needs.  Response: Notify maintenance personnel on-site. | Action: Aggregate maintenance data to determine patterns or recurring issues.  Response: Schedule preventative maintenance based on aggregated data. | Action: Maintain records of all maintenance activities in the cloud.  Response: Analyze maintenance data to optimize sensor deployment. |
| **Security and Access Control** | Action: Encrypt data on the device and ensure secure local communication.  Response: Implement local authentication measures. | Action: Ensure secure transmission of data to the cloud.  Response: Authenticate users accessing Fog layer data. | Action: Enforce strict access control and audit logs in the cloud.  Response: Ensure data privacy and security for sensitive information. |
| **Real-time Data Analysis** | Action: Perform initial analysis on sensor data to identify anomalies.  Response: Provide immediate feedback on sensor performance. | Action: Aggregate data from multiple sources to identify trends or issues.  Response: Enable improved accuracy in anomaly detection. | - |

**3. Based on the above table, identify the sensors and actuators required**

**Sensors**:

* **Smoke Sensors**: Detect smoke presence in the environment.
* **Gas Sensors**: Measure concentrations of specific gases (e.g., carbon monoxide, methane).
* **Flame Detectors**: Identify flames using infrared or ultraviolet light.
* **Sensor Performance Monitors**: Monitor the status and performance of the smoke, gas, and flame sensors.
* **Authentication Sensors**: Enable secure access control for users.

**Actuators**:

* **Audible Alarms**: Emit sound alerts for immediate hazard notification.
* **Visual Indicators**: Use flashing lights to provide visual alerts.
* **Sirens**: Trigger sound alerts on-site when hazards are detected.
* **Display Screens**: Present real-time data and alerts for on-site personnel.
* **Maintenance Alerts**: Notify maintenance personnel of any sensor performance issues.

**4. Identify the communication protocols required.**

**Edge Layer**:

* **MQTT**: For real-time data transmission and alerts.
* **CoAP**: For communication between constrained devices and the Fog layer.
* **Bluetooth Low Energy (BLE)**: For local, short-range communication with wearable devices.
* **Zigbee**: For connecting sensors in a low-power, mesh network.

**Fog Layer**:

* **HTTP/HTTPS**: For secure communication with the Cloud.
* **WebSocket**: For real-time updates between Fog and Cloud.
* **LoRaWAN**: For long-range communication, especially in larger industrial settings.

**Cloud Layer**:

* **RESTful APIs**: For interaction with Cloud services.
* **AMQP**: For reliable messaging and data queuing.
* **HTTPS**: For secure data transfer and access to Cloud services.