KONGU ENGINEERING COLLEGE

PERUNDURAI, ERODE-638052

DEPARTMENT OF INFORMATION TECHNOLOGY

20ITL61

INTERNET OF THINGS LABORATORY

A PROJECT REPORT ON
DOOR SECURITY SYSTEM USING IR SENSOR

Submitted By

NAME OF THE CANDIDATE

HARI PRASATH P N
KANISHKAR K M
KAVIN PRAKASH M
MOHAN BABU R

Register Numbers

21ITR037
21ITR047
21ITR051
21ITR063

KONGU ENGINEERING COLLEGE

PERUNDURAI, ERODE-638052

DEPARTMENT OF INFORMATION TECHNOLOGY

20ITL61

INTERNET OF THINGS LABORATORY

A PROJECT REPORT ON

DOOR SECURITY SYSTEM USING IR SENSOR

Submitted By:

NAME OF THE CANDIDATES
HARI PRASATH P N
KANISHKAR K M
KAVIN PRAKASH M
MOHAN BABU R

Register Numbers
21ITR037
21ITR047
21ITR051
21ITR063

Faculty Incharge HoD/IT

Index

CHAPTER: 1 Rubrics for Assessment

Name of Concepts	Mark Allotted	Mark Given
IoT Level Identified	5	
Step 1: Purpose and Requirement Specification	30	
Step 2: Process Specification		
Step 3 Domain Model Specification		
Step 4 Information Model Specification		
Step 5 Service Specifications		
Step 6 IoT Level Specification		
Step 7 Functional View Specification		
Step 8 Operational View Specification		
Step 9 Device and Component Integration		
Step 10 Application Development		
Hardware Implementation/ Simulation Using Mobile/ Any other Online Circuit Modeling	15	
Software Implementation	10	
Cloud Technology Integration	10	
Styling and User Interaction	(10)	
Project Report	(10)	
Presentation	(10)	
	Total (100)	

CHAPTER 2
ABSTRACT

Door security systems represent a significant advancement in residential protection, leveraging Internet of Things (IoT) technologies to enhance safety, streamline monitoring, and provide homeowners with greater control over access to their homes. This comprehensive abstract delves into the realm of smart door security, highlighting its transformative impact on home safety and its role in delivering a secure and convenient living environment.

Door security systems have emerged as essential tools for modern households, revolutionizing traditional door security measures through the integration of IoT-enabled devices, advanced sensors, and intelligent analytics platforms. By utilizing real-time data collection and analysis, these systems empower homeowners to monitor their doors, manage access, and respond to potential threats with ease.

In a Door security setup, interconnected cameras, sensors, and smart locks are strategically installed around entry points to monitor key parameters such as motion, unauthorized access, and door status. These devices continuously gather data, which is transmitted to a central hub or cloud-based platform for processing and analysis. Through sophisticated algorithms and machine learning techniques, this data is transformed into actionable insights, allowing homeowners to proactively address security concerns and automate door management.

A key feature of Door security systems is their ability to facilitate remote monitoring and control. Homeowners can access real-time data and insights from anywhere using mobile apps or web-based interfaces, allowing them to manage door locks, view live camera feeds, and receive notifications about door activity. This flexibility enhances security and convenience, providing the ability to control access remotely and monitor entry points in real time.

Moreover, Door security systems offer scalability and adaptability to changing household needs. Additional sensors, cameras, and devices can be easily integrated into the existing setup as required, ensuring comprehensive protection at all entry points. Compatibility with other smart home technologies, such as lighting, thermostat, and security alarms, creates opportunities for seamless home automation and a more interconnected living experience.

In summary, Door security systems represent a shift in residential protection, combining IoT technologies with advanced analytics to deliver safety, efficiency, and convenience. By embracing these innovative solutions, homeowners can achieve enhanced door security, greater control over access, and a heightened sense of safety in their homes.

CHAPTER 3
IOT LEVEL IDENTIFIED

Exploring the various levels of IoT integration within smart door security systems is essential for understanding their capabilities and how they optimize safety and convenience for homeowners. This chapter examines the different levels of integration within smart door security systems and their impact on access control, monitoring, and overall home security.

At Level 1 of IoT integration in smart door security systems, the emphasis is on foundational features such as basic monitoring and control. Entryway sensors and smart locks collect data on door activity, including open and closed statuses. This data is transmitted to a local controller via wired connections, allowing homeowners to monitor door status locally. However, Level 1 systems offer limited remote access and basic functionality without advanced analytics or remote control features.

Moving to Level 2, smart door security systems incorporate wireless communication technologies to enhance connectivity and flexibility. Sensor nodes and smart locks communicate wirelessly with a central hub, enabling seamless data aggregation and remote monitoring. This integration allows homeowners to receive alerts about door activity on their mobile devices, providing greater awareness and responsiveness. However, Level 2 systems may not offer comprehensive analytics or predictive insights.

At Level 3, smart door security systems reach optimal integration with cloud-based platforms and advanced analytics. Sensor data is sent in real-time to cloud servers, where it undergoes in-depth analysis for predictive insights and real-time monitoring. This level of integration empowers homeowners with proactive notifications about potential security risks and allows them to manage their door security remotely from any location. Level 3 systems provide the highest level of access control, including managing smart locks and viewing live camera feeds.

In summary, the level of IoT integration in a smart door security system depends on a homeowner's specific needs and the desired functionalities. While Level 1 systems offer basic monitoring, Level 2 and Level 3 systems introduce advanced features such as wireless connectivity, real-time alerts, and cloud-based analytics. By evaluating these options, homeowners can choose the most appropriate level of IoT integration to optimize door security and enhance the safety of their home.

CHAPTER 4

IOT DESIGN

Designing a smart door security system leveraging IoT technologies requires a systematic approach to ensure its effectiveness, reliability, and scalability. This section outlines the key steps involved in creating such a system, covering aspects such as purpose and requirement specification, process specification, domain model specification, information model specification, service specifications, and IoT level specification.

1. Purpose and Requirement Specification:

The design process starts with clearly defining the objectives and requirements of the smart door security system. This includes identifying the types of access control needed, the specific types of sensors and cameras to be used, desired user features such as alerts and notifications, and compliance with security and privacy standards. Understanding these requirements is crucial for shaping the system's scope, functionality, and performance criteria.

2. Process Specification:

In this phase, the operational workflow and processes of the smart door security system are outlined. This includes defining how sensors and smart locks will function, the sequence of activities for access control and monitoring, and the system's response to potential security threats. Additionally, protocols for handling security events, generating alerts, and providing notifications are established to ensure quick and effective responses to security incidents.

3.Domain Model Specification:

The domain model specification defines the various components and their interactions within the smart door security system. This includes sensors, smart locks, cameras, user interfaces, and any external devices or systems that interact with the security system. Crafting a comprehensive domain model ensures a robust system architecture that aligns with the system's goals and requirements.

4.Information Model Specification:

In this phase, the smart door security system defines its data structure and communication protocols. This includes deciding how data will be organized and transmitted, considering efficiency and compatibility with existing smart home systems. Data collection, transmission, storage, and analysis methods are established to ensure seamless integration and smooth operation. Interoperability standards are also considered to facilitate communication with third-party systems and devices.

5. Service Specifications:

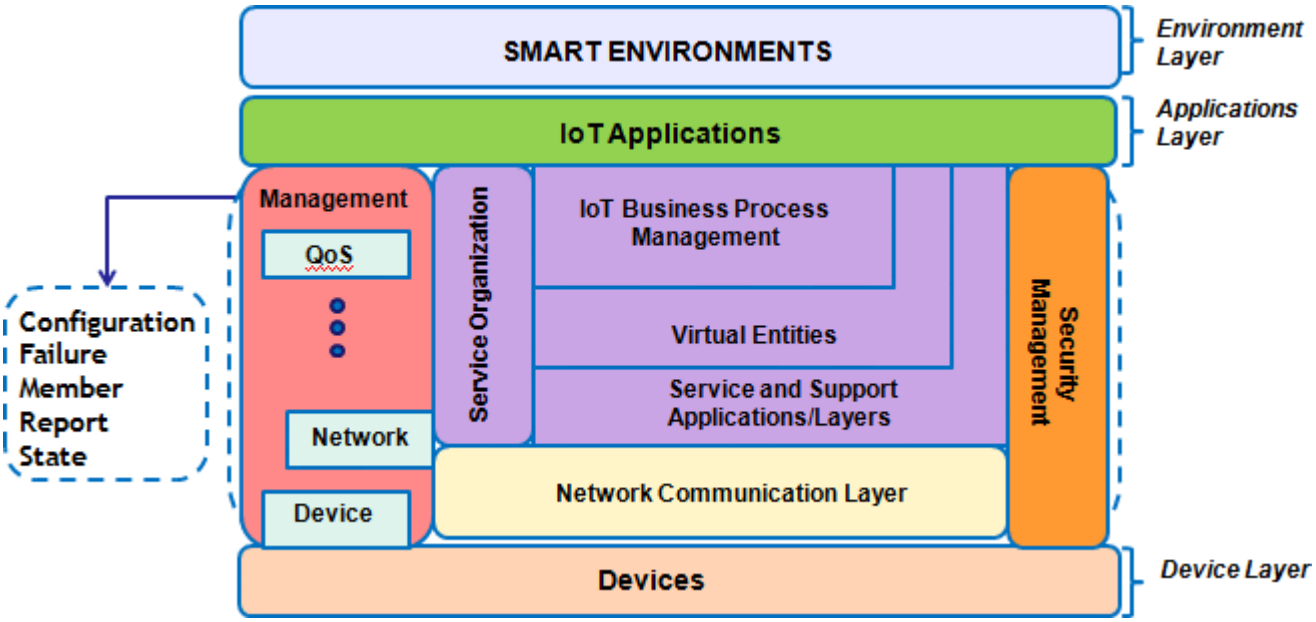
Service specifications outline the functionalities and features offered by the smart door security system. These include access control, real-time monitoring, remote lock/unlock capabilities, and customizable alerts and notifications. Defining these services aligns the system with homeowner preferences and integrates it seamlessly into daily routines for greater convenience and enhanced security.

1. IoT Level Specification:

Finally, the appropriate IoT level for the smart automation system is determined based on factors like complexity, connectivity, and functionality requirements. This assessment considers the size of the facility, environmental intricacies, and the desired extent of monitoring and control. Choosing the right IoT level ensures that the system is custom-fit to effectively meet safety and operational needs.

By adhering to these design steps, developers craft a resilient and effective smart automation system. This methodical approach guarantees alignment with organizational goals, regulatory standards, and industry benchmarks, thereby optimizing workplace efficiency and safety.

4.1 Step 1: Purpose and Requirement Specification



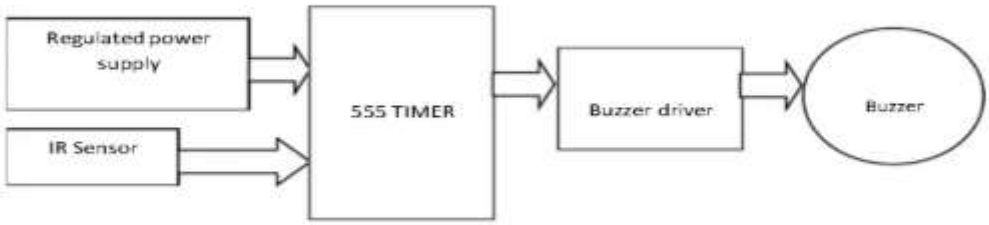
Purpose and requirement specification is the foundational step in designing a smart door security system leveraging IoT technologies. This phase involves clearly defining the objectives, goals, and functional requirements of the system to ensure its effectiveness in providing comprehensive door security. The following aspects are typically addressed during this phase:

1. Identification of Objectives: The first step involves pinpointing the core objectives of the smart door security system. This includes understanding its primary role, whether it's to enhance home safety, control access, monitor entry points, or integrate with other smart home features

such as lighting and security cameras. By determining these objectives, you can establish a clear framework for the system's overall functionality and desired outcomes.

Step 2: Process Specification

BLOCK DIAGRAM



Process specification in the design of a smart door security system involves outlining the operational workflow and processes to ensure efficient and effective monitoring and response to potential security threats. This phase focuses on defining the sequence of activities, data collection methods, processing algorithms, and alarm generation mechanisms. The following aspects are typically addressed during this phase:

1.Data Collection Methodology: The initial step involves defining how various data points will be collected within the smart door security system. This includes determining the placement and distribution of sensors and cameras based on factors such as entry point locations, high-traffic areas, and potential blind spots.

2. Sampling Frequency: The frequency at which data points are sampled and recorded is determined by factors such as the level of security required, the presence of frequent entry and exit, and the responsiveness of the system. Higher sampling frequency can enhance real-time monitoring and quick response to security events.

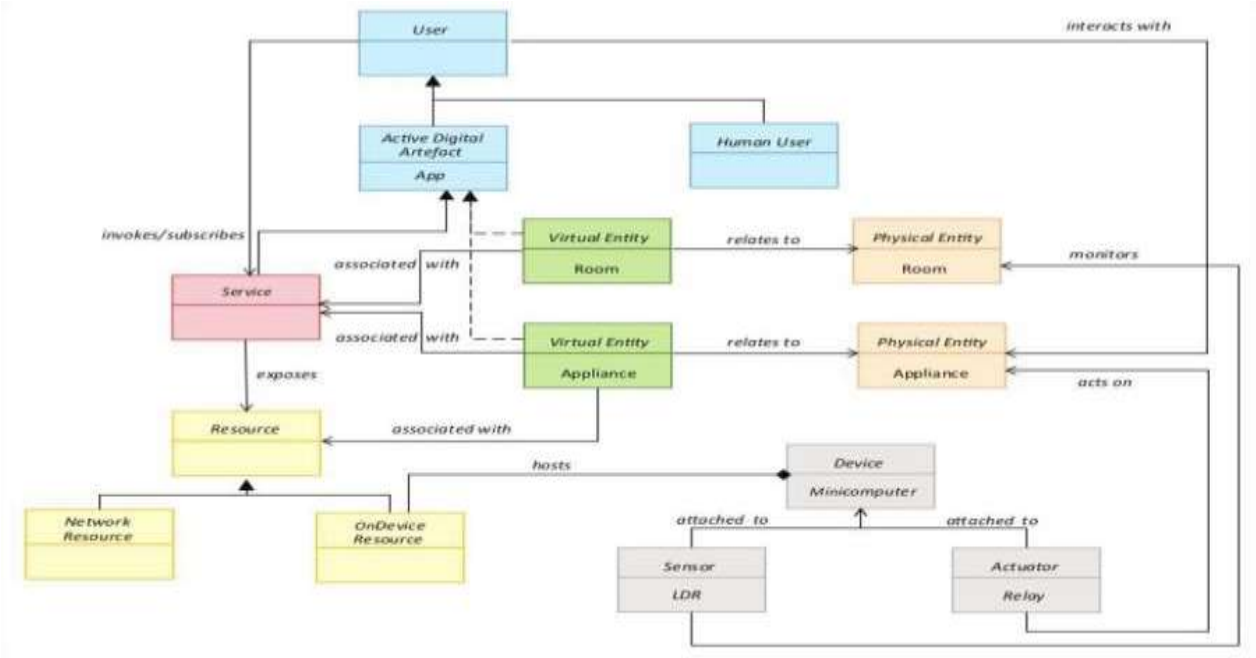
3. Data Processing Algorithms: Algorithms for processing the collected data are specified within the smart door security system to analyze entry and exit activity, recognize patterns, and detect potential security threats. This may include motion detection, facial recognition, or threshold-based anomaly detection.

4. Alarm Generation and Notification: Protocols are established for generating alarms and alerting relevant individuals in the event of security incidents. This includes setting alarm thresholds for various parameters, defining triggers such as unauthorized access or unusual activity, and determining notification methods (e.g., mobile notifications, alerts, or audible alarms).

5.Incident Management Protocol: The system establishes comprehensive protocols for managing detected incidents within the smart door security framework. This includes defining roles and responsibilities, outlining escalation procedures, and specifying responses such as locking doors, activating alarms, or contacting authorities as needed.

6.Testing and Validation: The specified operational processes within the smart door security system undergo thorough testing and validation to ensure their effectiveness in detecting and responding to incidents. This includes conducting simulated break-in scenarios, testing alarm triggers and response procedures, and evaluating system performance under various conditions.

Step 3: Domain Model Specification



Domain model specification in the design of a smart door security system involves defining the various components and their interactions within the system. This phase focuses on creating a comprehensive representation of the system's domain, including sensors, smart locks, cameras, communication protocols, user interfaces, and any external systems or devices that interact with the system. The following aspects are typically addressed during this phase:

1. Identification of Components: The initial step involves identifying and listing all components that make up the smart door security system. This includes door sensors, smart locks, cameras for monitoring, communication modules for data transmission, and any other relevant hardware or software elements that contribute to the system's functionality.

2. Definition of Interactions: Specifications for interactions between different components within the system are established. This includes defining communication protocols, data formats, and interfaces to

ensure seamless integration and interoperability among sensors, locks, and other devices.

3. System Architecture: The overall architecture of the smart door security system is outlined, encompassing the physical arrangement of sensors, locks, and communication infrastructure throughout the property. This may include creating system diagrams or architectural blueprints to visualize the system's layout and how components are interconnected.

4. Functional Decomposition: Each component's functionality within the system is broken down into smaller, manageable tasks. This involves dividing complex functions into simpler, modular components that can be implemented, tested, and maintained more effectively.

5. User Interfaces and Human-System Interaction: Consideration is given to the design of user interfaces and interactions between users and the system. This includes defining user roles, permissions, and access levels, as well as designing intuitive interfaces for monitoring, configuring settings, and responding to alerts within the smart door security system.

6. Error Handling and Fault Tolerance: Mechanisms for error handling, fault detection, and recovery are specified to enhance the system's robustness and reliability. This involves defining error codes, diagnostic messages, and procedures for detecting and responding to system failures or anomalies.

7. Integration with External Systems: If the smart door security system interfaces with external systems or devices, such as other smart home technologies, communication protocols and interfaces for integration are defined. This ensures seamless interoperability and data exchange between the door security system and other systems within the home.

Step 4: Information Model Specification

In the design of a smart door security system, the information model specification focuses on defining the data structure, communication protocols, and information flow within the system. This phase is essential for ensuring seamless data collection, transmission, storage, and analysis to support real-time monitoring and decision-making. The following aspects are typically addressed during this phase:

1**. Data Structure Definition:** The first step is to define the structure of the data collected by the smart door security system. This includes specifying the types of data to be collected, such as door status (open/closed/locked), sensor readings (e.g., motion, sound), timestamps, and any additional metadata such as user IDs or device IDs. The data structure is designed to facilitate efficient storage, retrieval, and analysis of sensor data.

2. Data Encoding and Formats:Protocols for encoding and formatting data are specified to ensure interoperability and compatibility with different components and systems. Common data formats such as JSON, XML, or CSV may be used depending on the system's requirements and its integration with external systems.

3. Communication Protocols: The protocols for data transmission between sensors, smart locks, controllers, and other system components are defined. This includes specifying communication protocols such as TCP/IP, MQTT, or HTTP, as well as data exchange formats and message schemas.

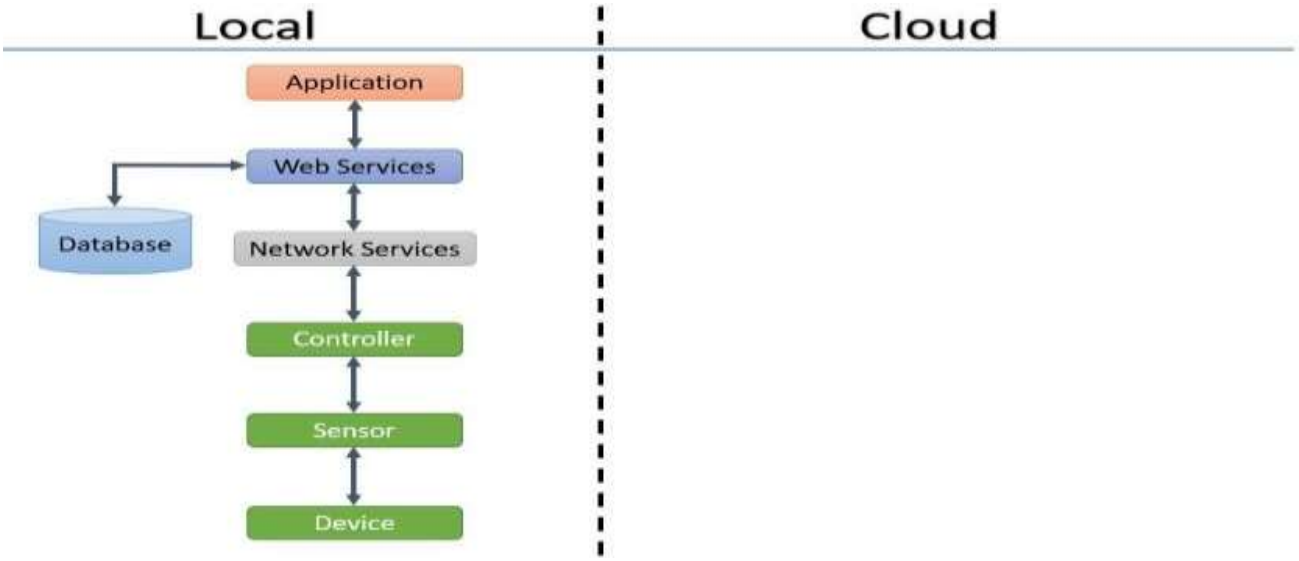
4. Data Transmission Methods: Methods for transmitting data from sensors to a centralized control hub or cloud-based platform are established. This may involve using wired or wireless communication technologies such as Ethernet, Wi-Fi, Bluetooth, or Zigbee, depending on the range, bandwidth, and reliability requirements of the system.

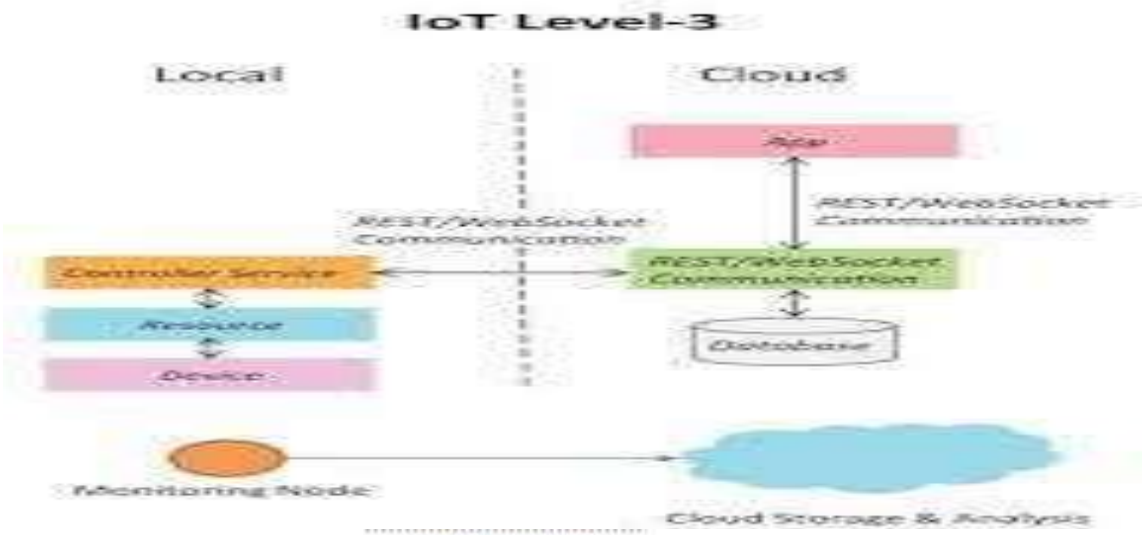
5. Data Storage and Retention Policies: Policies for storing and retaining sensor data are defined to ensure compliance with regulatory requirements and operational needs. This includes specifying storage duration, data archival procedures, and data encryption methods to protect sensitive information.

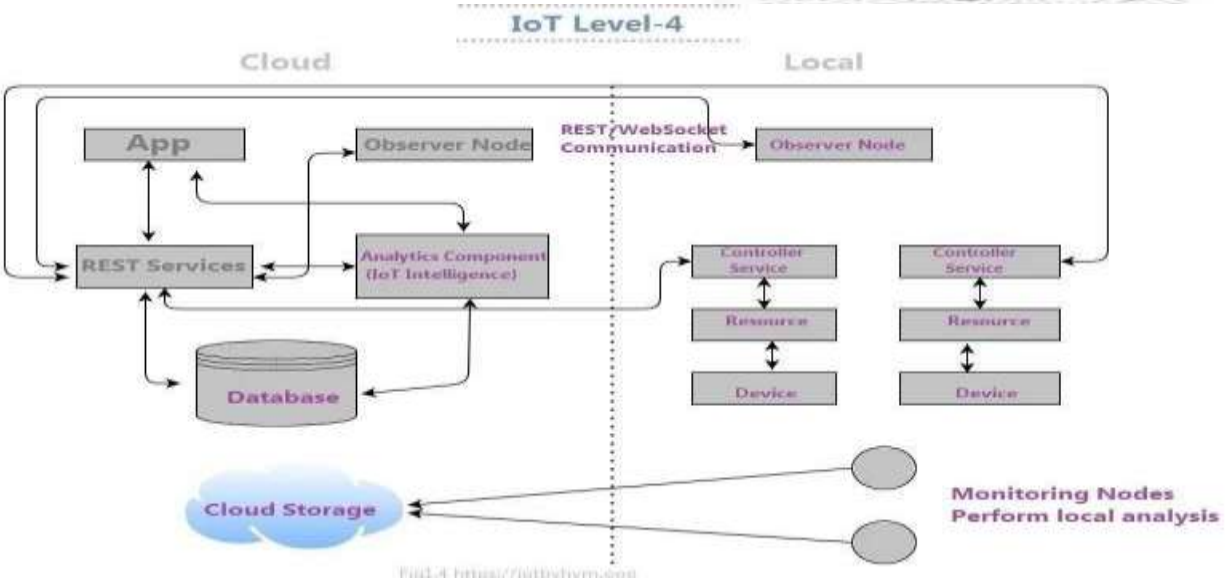
6. Data Analysis and Processing Pipelines: Pipelines for processing and analyzing sensor data are outlined to derive actionable insights and detect anomalies or patterns indicative of security threats. This may involve implementing algorithms for real-time analytics, anomaly detection, or trend analysis to support decision-making and response strategies.

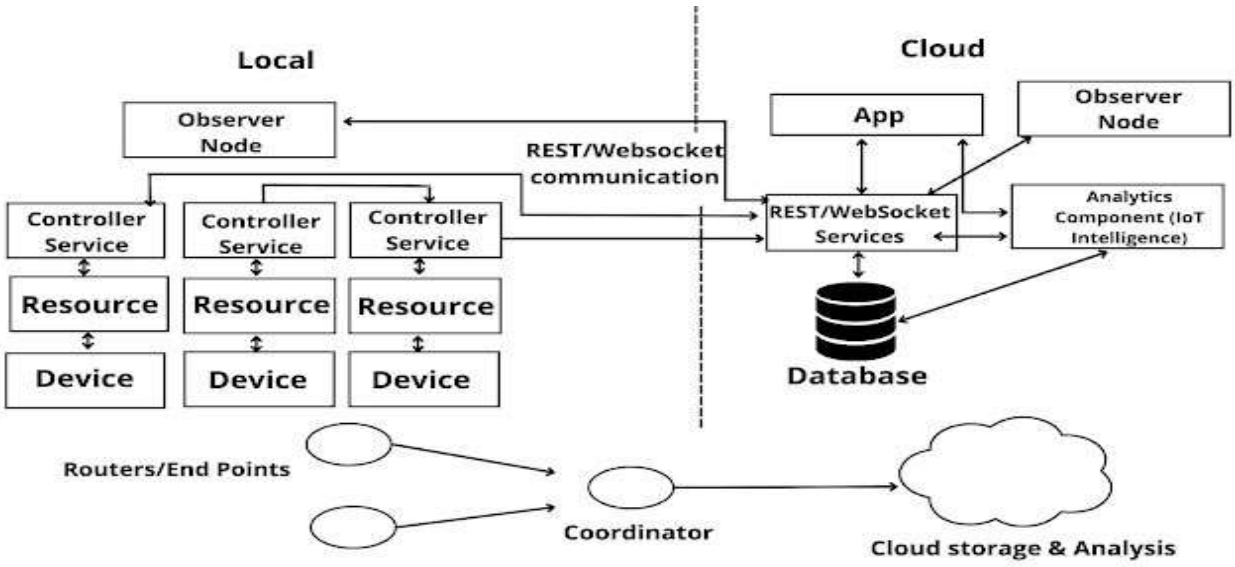
7. Integration with Analytics Platforms: If the smart door security system integrates with external analytics platforms or cloud services for data analysis, the protocols and interfaces for data exchange are specified. This enables seamless integration with advanced analytics tools and platforms for enhanced data visualization, reporting, and decision support.

Step 5: IoT Level Specification




IoT Level-3
Local
Cloud
App
REST/WebSocket Communication
Controller Service
REST/WebSocket Communication
Resource
Device
Database
Monitoring Node
Cloud Storage & Analysis


IoT Level-4
Cloud
Local
App
Observer Node
REST/WebSocket Communication
Observer Node
REST Services
Analytics Component (IoT Intelligence)
Controller Service
Controller Service
Resource
Resource
Device
Device
Database
Cloud Storage
Monitoring Nodes
Perform local analysis


Local
Cloud
Observer Node
REST/Websocket communication
App
Observer Node
Controller Service
Controller Service
Controller Service
REST/WebSocket Services
Analytics Component (IoT Intelligence)
Resource
Resource
Resource
Device
Device
Device
Database
Routers/End Points
Coordinator
Cloud storage & Analysis

In the design of a smart door security system, IoT level specification involves determining the appropriate level of IoT integration based on the system's complexity, connectivity requirements, and desired functionality. This phase ensures that the system leverages IoT technologies effectively to meet safety objectives, operational needs, and homeowner preferences. The following aspects are typically addressed during this phase:

1. Assessment of System Requirements: The first step is to assess the specific requirements of the smart door security system, including the size and layout of the property, the complexity of the security environment, and the desired level of monitoring and control. This helps identify the key factors that will influence the selection of the IoT level.

2. Evaluation of IoT Capabilities: The capabilities and features offered by different IoT levels are evaluated to determine their suitability for meeting the system requirements. This includes assessing factors such as wireless connectivity, data processing capabilities, remote access, scalability, and interoperability with other smart home systems.

3. Selection of IoT Level: Based on the assessment of system requirements and evaluation of IoT capabilities, the appropriate IoT level is selected for the smart door security system. This may range from basic IoT capabilities for simple monitoring and data collection (e.g., Level 1) to advanced IoT integration for real-time monitoring, analytics, and remote management (e.g., Level 3).

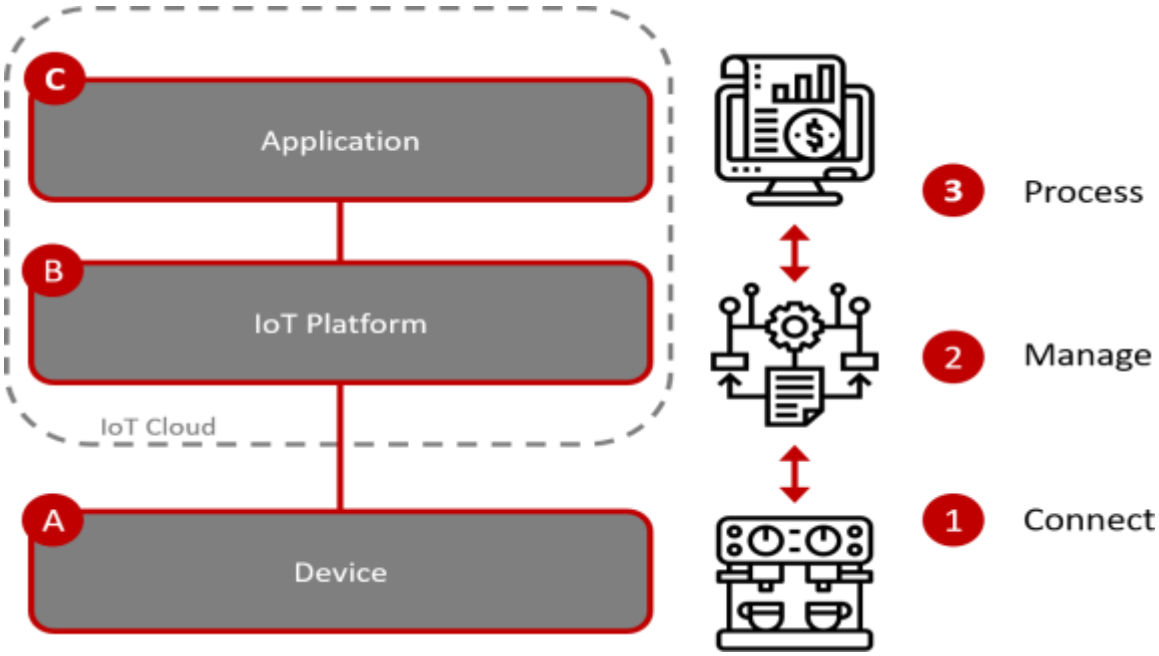
4.Consideration of Cost and Complexity:The cost and complexity associated with each IoT level are considered to ensure that the selected level aligns with the homeowner's budget and technical capabilities. This involves weighing the benefits of advanced features against the costs and potential challenges of implementation and maintenance.

5. Scalability and Future Expansion:The scalability of the selected IoT level is evaluated to ensure that the system can accommodate future expansion or changes in requirements. This includes assessing the ability to add additional sensors, devices, or functionalities as needed without significant modifications to the existing infrastructure.

6. Risk Assessment: Potential risks and challenges associated with the selected IoT level are identified and mitigated to ensure the successful implementation and operation of the smart door security system. This may involve addressing concerns such as data security, reliability of wireless connectivity, and compatibility with existing home infrastructure.

7. Documentation and Communication:The selected IoT level is documented and communicated to stakeholders, including homeowners, maintenance personnel, and any service providers. This ensures alignment and understanding of the system requirements, capabilities, and expected outcomes

Step 6: Operational View Specification



Operational view specification in the design of a smart door security system involves defining how the system functions in various real-world scenarios, including normal operation, abnormal conditions, and emergency situations. This phase outlines how the system behaves and responds in these different operational contexts to ensure home security, safety, and user experience. The following aspects are typically addressed during this phase:

1. Normal Operation: The behavior of the system during normal operation is described, including routine monitoring of door access, verification of authorized users, and data collection. This includes specifying how components like smart locks, cameras, and sensors interact to facilitate seamless day-to-day security.

2.Abnormal Conditions: The system's response to abnormal conditions, such as unauthorized access attempts or tampering, is outlined. This includes defining alarm triggers, notification mechanisms, and response procedures for alerting homeowners and initiating security measures.

3. Emergency Situations:The system's behavior during emergency situations, such as home invasions or fire alarms, is described. This includes specifying emergency response protocols, automatic door locking mechanisms, and actions to ensure the safety of occupants.

4. Fault Tolerance and Redundancy: Mechanisms for fault tolerance and redundancy are specified to ensure the reliability and availability of the system. This includes defining backup power sources,

redundant communication channels, and failover procedures to maintain continuous operation during component failures or disruptions.

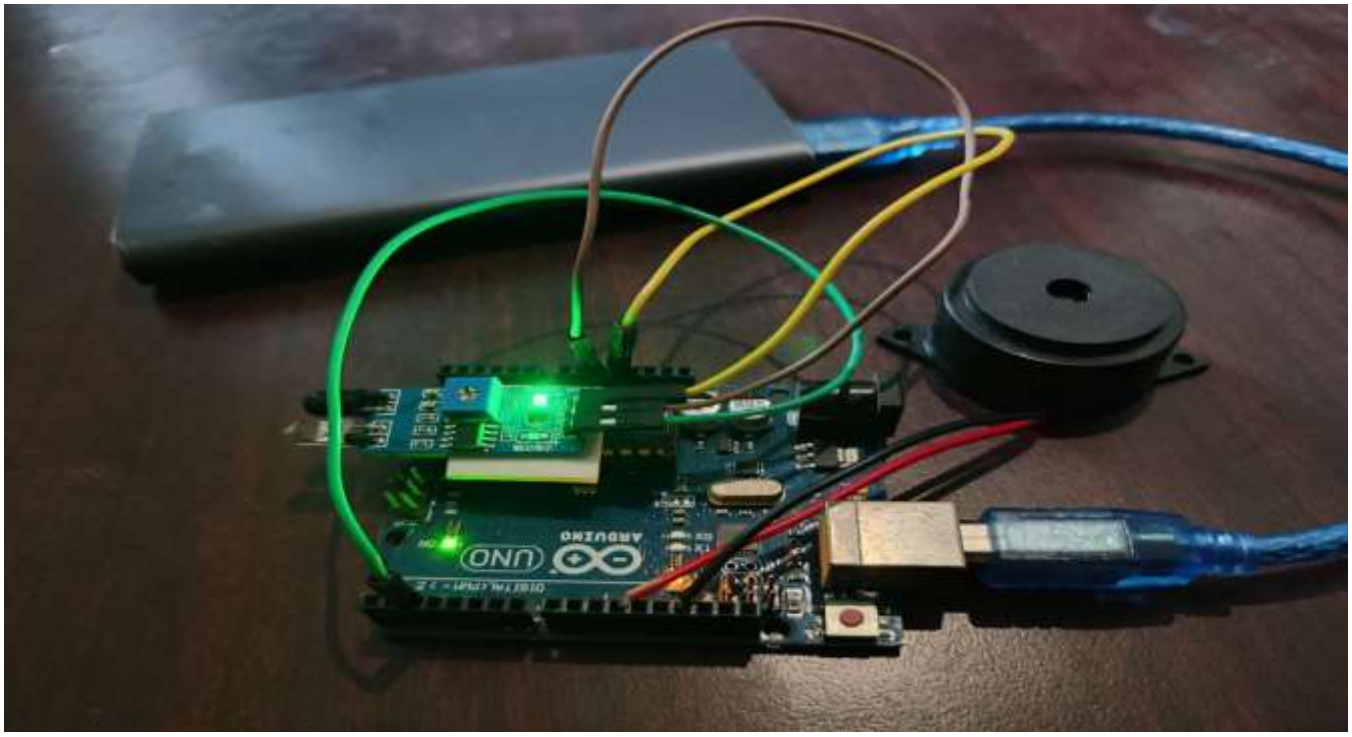
5. Scalability and Performance: The system's scalability and performance characteristics are evaluated to ensure it can handle increasing user loads and changing security needs. This includes assessing factors such as response time, data processing speed, and the ability to scale up with additional smart home devices.

6. Resource Management: The management of system resources, such as power consumption, network bandwidth, and computational resources, is outlined to optimize system performance and efficiency. This includes defining strategies to manage resource usage and ensure the system's long-term sustainability.

7. Integration with Operational Processes:Integration points and interfaces with existing smart home processes and workflows are identified to ensure seamless interoperability. This includes specifying data exchange protocols and integration points with other smart devices or home automation systems.

8. Testing and Validation Scenarios:Scenarios for testing and validating the system's operational behavior are defined to ensure it performs as intended under various conditions. This includes creating test cases, simulations, and scenarios to evaluate the system's response to different operational challenges and emergencies.

Step 7: Application Development



Implementing door security using an Arduino Uno, an IR sensor, and a buzzer offers a simple yet effective approach to securing an entrance. The Arduino Uno microcontroller serves as the core of the system, processing input from the IR sensor and controlling the buzzer. The IR sensor detects movement by measuring infrared radiation emitted by objects or individuals in its range. When movement is detected, the Arduino triggers the buzzer to emit an audible alarm, alerting the user to potential unauthorized entry.

The setup begins with wiring the IR sensor and the buzzer to the Arduino Uno. The sensor's signal output is connected to a digital input pin on the Arduino, while the buzzer is connected to a digital output pin. Both the IR sensor and the buzzer receive power from the 5V and ground pins on the Arduino. Once the hardware connections are established, the next step involves programming the Arduino with a sketch that continuously reads the signal from the IR sensor. If the sensor detects movement, the sketch activates the buzzer.

Configuring the IR sensor may involve adjusting its sensitivity and range to effectively monitor the desired area near the door without triggering false alarms. After programming the Arduino and configuring the sensor, the system should be tested by simulating movement near the door. The buzzer should sound an alarm when the IR sensor detects movement, confirming that the system is working as intended.

Placement of the IR sensor is crucial for optimal performance. It should be positioned to effectively monitor the area around the door without interference or obstructions. Additionally, ensuring a stable power supply for the system is essential, whether through a USB connection or a suitable battery pack. The buzzer should be loud enough to alert the user in other parts of the house, and the system can be integrated with other smart home devices or additional security measures for enhanced protection.

While the initial setup is straightforward, ongoing adjustments may be necessary to fine-tune the sensitivity and range of the IR sensor. This ensures that the system operates reliably and effectively over time. Considerations such as user response to the alarm and potential integration with other security systems can also enhance the overall security setup.

Implementing door security with an Arduino Uno, IR sensor, and buzzer is a cost-effective and efficient method to secure an entrance. This approach provides real-time monitoring and immediate audible alerts, enhancing safety and security. The system can be customized and expanded to meet specific security needs, making it a versatile solution for various environments. With careful setup and testing, this security system can provide reliable protection for your home or business.

CHAPTER 5
GIT HUB LINK

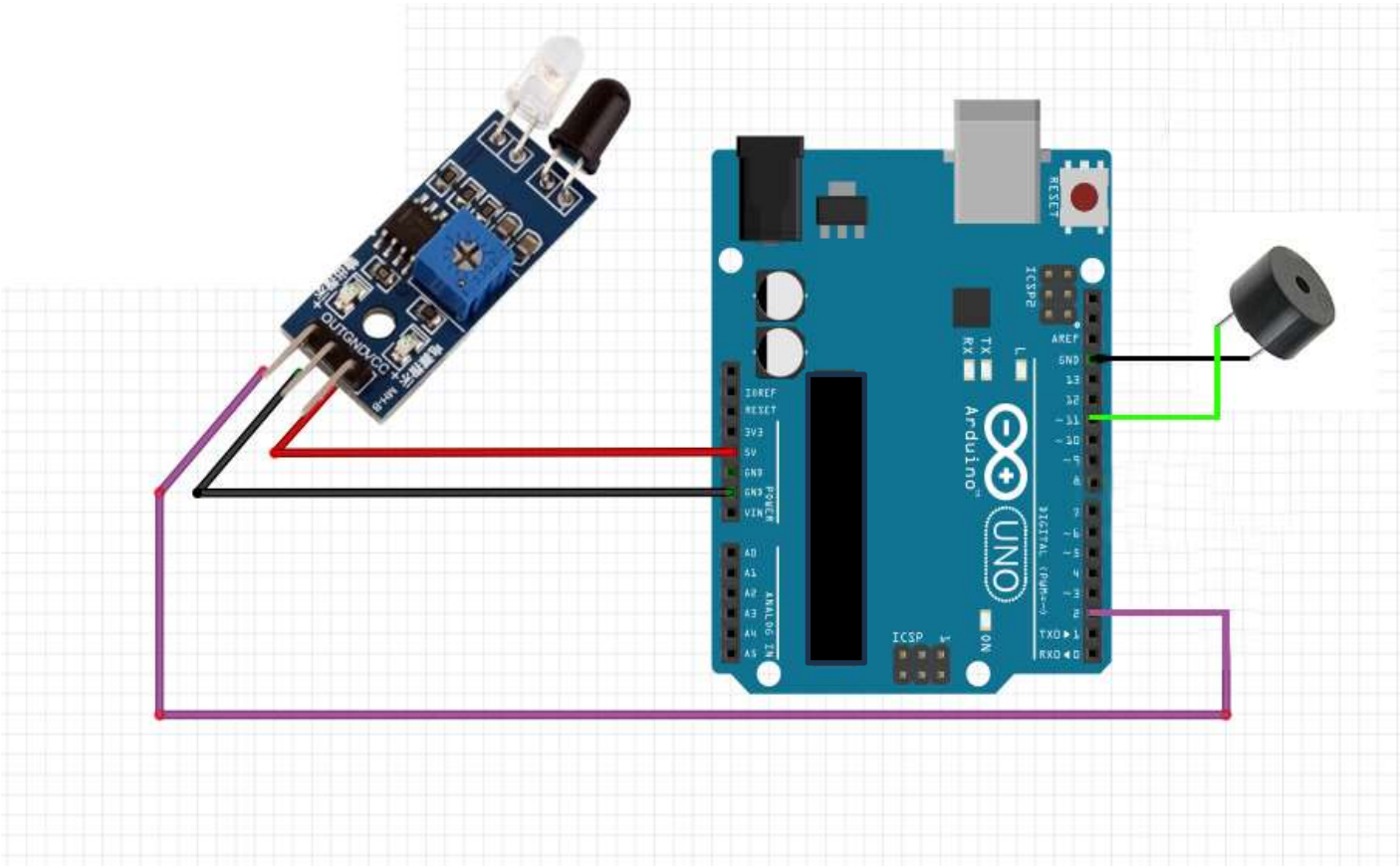
21ITR037: https://github.com/hariprasath-0ffl/Door-security-System-IOT

21ITR047: https://github.com/kanish-km/Door-security-System-IOT

21ITR051: https://github.com/kavinprakash05/Door-security-System-IOT

21ITR063: https://github.com/Mohanbabu07/Door-security-System-IOT

CHAPTER 6
HARDWARE SCREENSHOT



CHAPTER 7
CODING

```
byte ir_sensor = 2;
byte buzzer = 11;

void setup()
{
 pinMode(ir_sensor, INPUT);
 pinMode(buzzer, OUTPUT);
}

void loop()
{
 int sensor_state = digitalRead(ir_sensor);

 if(sensor_state == LOW)
 {
  digitalWrite(buzzer, HIGH);
 }


}
```

CHAPTER 8

RESULT AND CONCLUSION

RESULT:

The door security system successfully monitored and managed access to the designated areas, providing operators with real-time data on door status and potential unauthorized entry. Through its network of sensors and interconnected devices, the system facilitated proactive decision-making, enabling swift action in response to any security breaches.

CONCLUSION:

The implementation of a door security system has proven to be effective in enhancing safety and controlling access within various environments. By leveraging interconnected devices and instant alerts, the system allows for proactive monitoring and immediate responses to potential threats. This setup not only reduces the risk of security incidents but also contributes to improved overall safety and peace of mind. Moreover, the system's scalability and flexibility make it adaptable to different settings, including residential, commercial, and industrial properties. Investing in smart door security systems is essential for ensuring the safety of people and assets while supporting regulatory compliance and efficient resource management.

CHAPTER 10
REFERENCES

https://www.researchgate.net/publication/327935942_Security_System_using_Arduino

https://www.scribd.com/document/433315778/Ir-Sensor-Based-Home-Security-System

DOOR SECURITY SYSTEM USING IR SENSOR
https://www.youtube.com/watch?v=-h_pS6YIosc