Department of Computer Science and Engineering

CSB4232 – DESIGN PROJECT WITH IOT

CONTACTLESS DOORBELL SYSTEM

Review-1

Abirajah P A 21113069

Dharshan R E 21113049

Harish Jayaram S S 21113050

SUPERVISORS

Dr.R.Logeshwari, Professor

1. Executive Summary:

-An overview of the project:

The Contactless Doorbell System with Local Cloud Server is a creative and practical solution designed to enhance security and convenience in residential and commercial settings. This system utilizes an ESP32-CAM device to detect human presence at the door, capture images, and provide real-time remote monitoring through the Blynk app. The local cloud server, hosted on a Windows platform, ensures secure and private storage of captured images while allowing users to interact with the system**.**

- Summary of key findings and recommendations.

-- Summary of key findings

Enhanced security: The outdoor unit uses the IR sensor to detect the human presence alert the user by adding extra layer of security by notifying users of visitors even when they are not physically present.

User interaction: The blynk app enables a special feature to user by monitoring the person in front of door by capturing images and user can unlock door by using the app template.

Privacy and Data Control: The use of a local cloud server addresses privacy concerns associated with external cloud services. Images are stored securely on the local server, giving users complete control over their data.

Inspiration for Industry: The project's success showcases the potential of contactless doorbell systems with local cloud server integration. It provides a viable model for companies to develop similar solutions that prioritize user privacy and data control.

-- Recommendations:

Interface Enhancement: Continuously refine the user interface of the blynk app for seamless interaction and easy understanding of app.

User Education: Develop comprehensive user guides and video tutorials that explain how to set up, use, and troubleshoot the system. Educate users about best practices for maintaining security, including creating strong passwords and keeping software up to date.

Scalability Planning: Design the system with scalability in mind. Consider how the system will handle an increasing number of users, devices, and interactions. Ensure that the local cloud server and the app can accommodate growth without sacrificing performance or security.

Legal and Privacy Compliance: Research and adhere to relevant legal and privacy regulations in your region. Ensure that the system's data collection, storage, and usage comply with applicable laws, protecting both your users' data and your project from legal challenges.

Continuous Improvement: Regularly update the system's firmware, app, and server components to address bugs, enhance security, and introduce new features. Communicate these updates to users and make the process as seamless as possible.

2. Introduction:

--Background information on IoT and its significance:

IoT, which stands for the Internet of Things, is a term that is used for connecting a bunch of devices we use in the real world to the internet. With IoT, the idea is to connect as many objects as possible to the internet When objects have internet connectivity, it means that they are capable of transferring information

The significance of IoT lies in its ability to make our lives more efficient, convenient, and interconnected by enabling devices to communicate, share data, and automate tasks, ultimately transforming the way we interact with our environment and enhancing various industries.

--Project Objective:

Create a contactless doorbell system that enhances security and convenience in residential and commercial settings.

Enable real-time remote monitoring of the doorstep through a smartphone app.

Capture images when human presence is detected and securely store them on a local cloud server.

Design an intuitive user interface within the Blynk app for viewing images and making informed decisions.

Prioritize privacy and data security by storing images locally and implementing robust security measures.

Inspire individuals and companies to develop IoT solutions with a focus on user privacy and data control.

--Project Scope:

Designing the hardware setup using the ESP32-CAM device, including integrating sensors for human presence detection and a buzzer for alerts.

Creating the Blynk app interface that enables remote monitoring, image viewing, and remote door unlock control.

Developing the local cloud server infrastructure on a Windows platform to securely store and manage captured images.

Ensuring the system's reliability, security, and user-friendliness through thorough testing and user feedback.

Demonstrating the system's effectiveness through scenarios involving human presence detection, image capture, remote monitoring, and remote door unlock.

Documenting the project's design, development process, and implementation, providing a comprehensive guide for users and developers interested in similar solutions.

3. Methodology

--Description of Research Methods:

The development of the Contactless Doorbell System with Local Cloud Server involves a systematic approach that encompasses diverse research methods to ensure the project's success. These methods contribute to the design, implementation, and validation of the system's functionalities and objectives.

Experimental Testing: Controlled tests validate sensor integration, buzzer functionality, and image capture.

User-Centric Approach: Real users engage with the Blynk app and system, offering feedback on interactions.

Security Assessment: Penetration tests identify vulnerabilities, encryption secures data, and access control ensures authorized use.

Iterative Development: Continuous adjustments are based on feedback, assessments, and experimental outcomes.

--Techniques used:

Hardware Integration: Integrate sensors (e.g., IR sensor) and components (e.g., buzzer) to create a cohesive system.

Software Development: Design a user-friendly Blynk app interface for remote monitoring and remote door unlock. Configure a local cloud server for image storage.

Practical Experimentation: Test human presence detection accuracy, image capture, and user interaction scenarios for system validation.

Security Assessment: Conduct penetration testing to identify vulnerabilities. Implement encryption for data transmission and access control mechanisms.

User Testing: Engage real users to interact with the Blynk app and system. Collect feedback to improve interface usability and functionality.

Iterative Refinement: Continuously refine hardware, software, and security measures based on user feedback, security assessments, and testing outcomes.

Ethical Considerations: Obtain user consent, prioritize data privacy, and ensure data handling aligns with ethical standards.

--Data collection procedures:

1.Human Presence Detection:

Perform controlled experiments with different scenarios to assess detection accuracy.

Record system responses, measuring accuracy and false positives/negatives.

2.Image Capture and Storage:

Simulate presence scenarios to trigger image capture.

Record captured image details, timestamps, and triggers.

Store images on the local cloud server and document the process.

3.Blynk App Usage:

Observe user interactions in the Blynk app.

Record image views, remote unlock attempts, and user feedback.

4.Security and Privacy:

Conduct penetration tests, document vulnerabilities, and potential exploits.

Implement encryption and access controls, recording their implementation.

4. Literature Review:

--Overview of existing literature and research on IoT and related technologies.

Literature review/Existing systems:

S. No	Title of the paper/System	Authors	Publication (Name of the Journal/Conference proceedings with Year)	Algorithm/Methodology adopted	Limitations
1.	Contactless IoT Doorbell	Ms.Shefali Raina, Vishwesh Pratap Singh, Md.Sajid Akhtar, Sidhant Ranjan Rishabh& Ajab Singh	22nd Journal of Emerging Technologies and Innovative Research(JETIR), 2022	• Ultrasonic sensor detects infrared changes • Using of Arduino UNO to send info to mobile	• Costlier than esp32 • Latency of information
2.	Doorbell System in Home Using IoT	B.Baron Sam1 , K. Purna Chander , K. Vinay & , A.Pio sajin	International Conference on Frontiers in Materials and Smart System Technologies,2021	• Utilizes protocols like MQTT or HTTP for efficient communication. • Fine-tune sensor parameters to reduce negatives and optimize	• High Power Consumption • Old Usage of sensor

S. No	Title of the paper/System	Authors	Publication (Name of the Journal/Conference proceedings with Year)	Algorithm/Methodology adopted	Limitations
3.	IoT & AI Based Smart Doorbell System	Prof. S.B. Sahu, Arati F. Paswan &, Kavita K. Tandi	International Journal Of Creative Research Thoughts,2021	• Employs deep learning models (e.g., CNN) to analyze captured images. • Set up cloud services (e.g., AWS, Azure) for data storage and processing.	• Lack of combability. • Security Risks
4.	A STUDY ON IOT SMART DOORBELLS	C.K Gomathy, & Devulapalli	International Journal Of Creative Research Thoughts,2021	• Classifies visitors, distinguishes between humans, animals, and objects. • Validate AI model accuracy, system responsiveness, and image analysis effectiveness.	• Bias in AI Models: AI models may inherit biases from training data, affecting visitor classification accuracy.

Research on IoT and related technologies:

The research landscape in IoT and related technologies is diverse and impactful, addressing various aspects of implementation and challenges:

Implementation Focus: Studies explore practical applications in domains like agriculture, smart cities, and healthcare, highlighting IoT's transformative potential.

Security and Privacy: Researchers tackle data security through encryption, authentication, and blockchain integration, while also addressing privacy concerns.

Edge and Fog Computing: Emerging paradigms like edge intelligence and fog computing are studied for their ability to enhance real-time data processing.

Interoperability and Standards: Standardization efforts seek to establish common protocols and semantic interoperability for seamless device communication.

Sustainability: IoT is leveraged for energy management and environmental monitoring, contributing to sustainable practices.

Key Concepts:

Human Presence Detection: The core concept involves using sensors like PIR to detect human presence, triggering actions such as image capture and alerts.

Real-Time Communication: IoT enables immediate communication between the doorbell system, user's app, and local cloud server, providing real-time updates.

Remote Interaction: Users can remotely interact with the doorbell system through a smartphone app to view images, unlock doors, and communicate with visitors.

Trends:

Enhanced User Experience: The trend is towards intuitive app interfaces that allow users to seamlessly navigate images, unlock doors, and interact with visitors.

Edge Processing: Utilizing edge computing, the doorbell system can process data locally, reducing latency and ensuring quick response times for alerts and image viewing.

Security Focus: Security measures are a prevailing trend, including secure data transmission, encrypted storage, and user authentication to protect against unauthorized access.

Challenges on IoT implementation:

Accurate Detection: Ensuring reliable human presence detection in various lighting conditions and angles to minimize false positives or negatives.

User Privacy: Managing captured images and user data while adhering to privacy regulations and gaining user consent for data collection.

Data Security: Implementing robust encryption protocols for data transmission and storage to prevent unauthorized access and potential breaches.

Compatibility: Ensuring compatibility with different smartphone platforms and devices to provide a consistent user experience.

Power Management: IoT devices like the contactless doorbell system must be energy-efficient to prolong battery life or ensure consistent operation if connected to a power source. Balancing functionality with power consumption is a challenge.

Network Reliability: Dependence on network connectivity introduces the risk of system downtime or delays in real-time alerts and image viewing. Ensuring a stable network connection is crucial for maintaining system responsiveness.

Environmental Factors: External elements like weather conditions, temperature variations, and physical obstructions can impact sensor performance and overall system reliability.

5. Design Requirements:

--Identification and explanation of the specific requirements for the IoT design project:

1.Accurate Human Presence Detection:

The system must reliably detect human presence at the door entrance.

Detection accuracy should minimize false positives and negatives.

2.Real-Time Alerts and Image Capture:

The system should send real-time alerts to the user's smartphone upon human presence detection.

Clear images of visitors should be captured and sent to the user's app.

3.Secure Data Transmission:

All data, including images and alerts, must be transmitted securely between the device and the user's app.

Encryption protocols should be implemented to ensure data privacy.

4.User Authentication and Access Control:

The app must feature robust user authentication methods to prevent unauthorized access.

5.Intuitive User Interface:

The smartphone app interface should be user-friendly and easy to navigate.

Users should be able to view images, unlock the door, and communicate with visitors effortlessly.

6.Compatibility and Interoperability:

The app should be compatible with various smartphone platforms (iOS, Android) for a seamless user experience.

7.Local Cloud Server Setup:

The local cloud server on the Windows platform must be configured to securely store captured images.

Data management and storage should adhere to privacy regulations.

8.Energy Efficiency:

Energy-efficient components and sleep modes can enhance battery life.

9.Remote Door Unlock Functionality:

The app should enable users to remotely unlock the door for authorized visitors.

This function should be secure and prompt a notification to the user.

10.Responsive Real-Time Communication:

Alerts, image viewing, and door unlock commands should have minimal latency for effective real-time communication.

11.User Privacy:

Captured images and user data should be handled with the utmost privacy and consent.

Data privacy regulations must be adhered to throughout the design and operation.

12.Scalability and Performance:

The system should be designed to handle multiple users, devices, and concurrent operations without degradation in performance

--Considerations for hardware, software, connectivity, security, and user experience:

1.Hardware:

Sensor Selection: Choose a reliable human presence detection sensor (e.g., PIR) that suits varying lighting conditions.

Camera Quality: Select a camera with appropriate resolution and field of view for clear visitor images. Physical Durability: Design the hardware to withstand environmental factors and potential tampering.

2.Software:

App Interface: Develop an intuitive smartphone app interface for image viewing, door unlocking, and communication.

Local Cloud Server Software: Choose suitable software (e.g., XAMPP) for the local cloud server setup on Windows.

Compatibility: Ensure the app works seamlessly on both iOS and Android platforms.

User Authentication: Implement strong user authentication methods to prevent unauthorized access.

3.Connectivity:

Network Options: Choose appropriate wireless technologies (Wi-Fi, Bluetooth) for connectivity between the doorbell system and user app.

Stable Connection: Prioritize network stability to ensure real-time alerts and image transmission.

4.Security:

Encryption: Implement encryption protocols (SSL/TLS) for secure data transmission between devices and the local cloud server.

User Data Protection: Ensure captured images and user data are securely stored and accessible only to authorized users

5.User Experience:

Ease of Use: Design the app interface with user-friendliness in mind, making image viewing, door unlocking, and communication intuitive.

Speed and Responsiveness: Minimize latency to provide real-time alerts, quick image loading, and remote door unlock.

6. System Architecture:

--Overview of the proposed system architecture for the IoT design:

The proposed system architecture for the IoT-based contactless doorbell system presents a comprehensive framework that integrates hardware, software, and connectivity components to create an efficient and user-friendly solution. This architecture is designed to provide accurate human presence detection, real-time communication, secure data handling, and seamless user interaction.

--Description of the components, their interconnections, and data flow.

1.Human Presence Detection Sensor:

Detects human presence at the door entrance using infrared technology.

Sends a signal to the microcontroller upon detection.

2.Microcontroller:

Receives signals from the human presence detection sensor.

Coordinates the system's operations based on the detected presence.

Activates the camera module for image capture.

3.Camera Module:

Sends the captured images to the microcontroller.

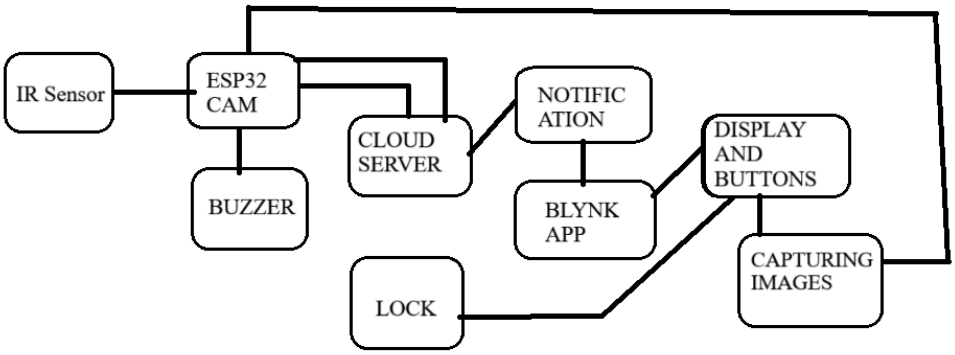
4.Local Cloud Server (Hosted on Windows Platform):

Acts as a centralized data repository for storing captured images securely. 5.Smartphone App (iOS/Android):

Receives real-time alerts and image data from the local cloud server.

Allows users to remotely unlock the door and communicate with visitors.

--System Architecture: Data Flow



7. Hardware Design:

--Detailed explanation of the hardware components and their specifications.

1.LED and Resistor (1 ohm):

LED (Light-Emitting Diode): An electronic component that emits light when current flows through it.

1 ohm Resistor: Limits the current passing through the LED to prevent damage and ensure proper operation.

Specifications: LED color, forward voltage, and current rating determine the resistor value.

2.12V Battery: A power source providing 12 volts for the system's operation.

Specifications: Battery capacity (Ah), and voltage stability.

3.Breadboard: A platform for prototyping circuits without soldering, facilitating component connections.

Specifications: Number of rows, columns, and power rails, compatibility with component sizes.

Buzzer: An audio output device that produces sound when voltage is applied.

Specifications: Operating voltage, sound frequency, current consumption, and sound level.

5.Solenoid Lock: An electromechanical device that uses an electrical current to generate a magnetic field, engaging the lock mechanism.

Specifications: Operating voltage, current draw, locking force, and compatibility with door types.

6.Push Button: A momentary switch used to initiate specific actions when pressed.

Specifications: Contact configuration (normally open or normally closed), actuation force.

7.Relay Module: An electromagnetic switch that controls high-power devices using low-power signals.

Specifications: Number of relays, contact rating, coil voltage, and compatibility with input signals.

8.UART TTL Module: A communication module facilitating serial communication between devices.

Specifications: Baud rate, voltage levels (TTL), communication range, and data format.

Detailed explanation of the hardware components and their specifications.

9.7805 IC Voltage Regulator: An integrated circuit that regulates voltage output to a stable 5 volts.

Specifications: Input voltage range, output voltage, current rating, dropout voltage.

10.25V 100uF Capacitor: An electrical component that stores and releases electrical energy.

Specifications: Voltage rating, capacitance, ESR (Equivalent Series Resistance).

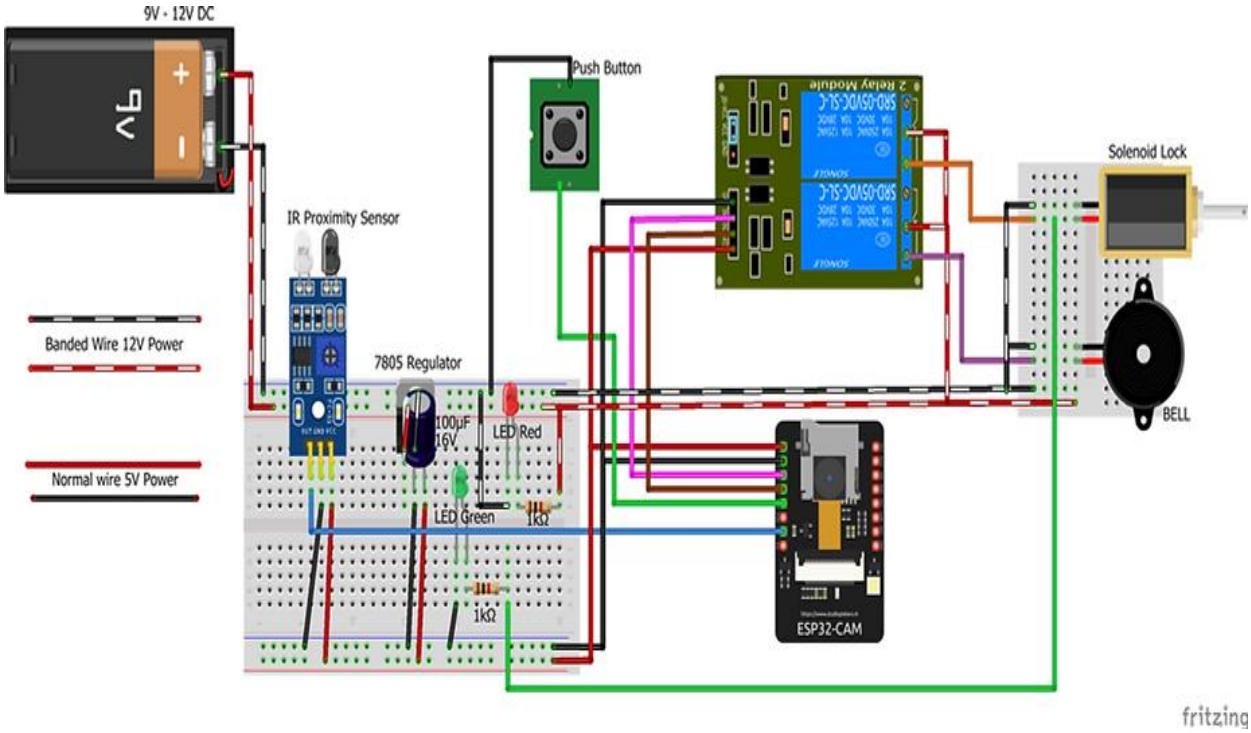
11.IR Proximity Sensor: A sensor that detects the presence of an object by emitting and receiving infrared light.

Specifications: Detection range, output type (analog or digital), response time.

12.ESP32-CAM: A versatile microcontroller combined with a camera module for image capture and processing.

Specifications: CPU speed, memory, camera resolution, Wi-Fi connectivity, GPIO pins.

--Circuit diagrams, schematics, and PCB layouts if applicable.



--Discussion of sensor selection, actuator integration, and power management

Sensor Selection:

Carefully choose the IR proximity sensor for accurate human presence detection based on its range, response time, and sensitivity.

Actuator Integration:

Integrate the solenoid lock and buzzer effectively with the microcontroller for remote door unlocking and timely user alerts.

Power Management:

Optimize energy consumption by using a 12V battery, voltage regulator, and power-saving techniques like sleep modes to ensure continuous and efficient system operation.

THANK YOU