International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**4**, pp.**41-46**, April **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org
ISSN: 2347-2693 (E)

Research Article

Bell Buddy: A Dual-Mode IoT-Based Smart Doorbell with Real-Time Facial Recognition and Intruder Alert System

Sivakami T.S.[1*], Jasmin Maria Binoy[2], Alphia Jose[3], Hredya Vijay[4]

[1,2,3,4]Dept. of CSE, Albertian Institute of Science and Technology, Ernakulam, India

*Corresponding Author:

Received: 16/Feb/2025; **Accepted**: 18/Mar/2025; **Published**: 30/Apr/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i4.4146

Abstract: In the evolving landscape of home automation, security remains a top priority. This paper presents "Bell Buddy," a dual-mode smart doorbell system designed to enhance residential safety through real-time image processing and IoT integration. The system operates in two distinct modes: Doorbell Mode and Intruder Detection Mode. In Doorbell Mode, when the bell is pressed, a notification is instantly sent to the user's mobile device, along with a captured image of the visitor for manual verification and remote access control. In Intruder Detection Mode, the system actively monitors for motion near the entrance and uses facial recognition algorithms to determine whether the detected individual is authorized or not. If an unknown face is identified, alerts are dispatched to both the user and predefined emergency contacts, while an audible alarm is triggered. The proposed system combines ESP32, Raspberry Pi, and cloud-based services for seamless real-time communication. The user interface is developed using React Native, while machine learning models trained using TensorFlow ensure accurate intruder detection. With end-to-end encryption and database integration, Bell Buddy offers an intelligent, efficient, and scalable solution for modern home security. The system has been evaluated on parameters such as recognition accuracy, notification speed, and reliability under varying environmental conditions.

Keywords: Smart Doorbell, IoT Security, Intruder Detection, Facial Recognition, Mobile Notification, ESP32, Raspberry Pi, Real-Time Image Processing, Home Automation, Deep Learning

1. Introduction

With the rapid advancements in smart home technologies, the demand for reliable, real-time, and intelligent security systems has significantly increased. Traditional doorbell systems lack the ability to authenticate visitors, leaving homeowners vulnerable to potential intrusions and unwanted access. While modern surveillance systems offer video recording and remote monitoring, they often fall short in providing immediate and automated responses based on visitor identity. To address these limitations, the integration of Internet of Things (IoT) devices with artificial intelligence (AI)-based recognition systems presents a promising direction for home security.

This paper introduces “Bell Buddy,” an intelligent, dual-mode smart doorbell system that leverages image processing and real-time alert mechanisms to ensure residential safety. The system operates in two primary modes: Doorbell Mode and Intruder Detection Mode. In Doorbell Mode, users receive real-time notifications along with the captured image of the visitor through a mobile application, enabling them to verify the visitor and remotely control the door lock. In Intruder Detection Mode, the system actively monitors the vicinity of the entrance using motion sensors. If movement is detected, it triggers a camera to capture the face of the individual and uses facial recognition to determine if the person is authorized. In case of an unknown face, the system sends alerts to the homeowner and emergency contacts, and activates an audible alarm.

The Bell Buddy system integrates ESP32 for hardware control, Raspberry Pi for facial recognition processing, and Firebase for real-time notifications. The mobile application is developed using React Native to ensure platform compatibility and ease of use. Advanced security protocols such as SSL, JWT, and AES encryption are incorporated to protect user data and communications.

This solution is cost-effective, scalable, and suitable for smart homes, hostels, and institutional buildings. Its ability to distinguish between known and unknown visitors in real-time makes it a proactive tool for security and convenience.

The rest of the paper is organized as follows: Section 2 discusses the related work in the domain of smart doorbell systems and IoT-based home security. Section 3 presents the system architecture and hardware/software components. Section 4 outlines the methodology and implementation strategy. Section 5 describes the experimental results and analysis. Section 6 provides a detailed discussion of findings. Section 7 concludes the study and highlights future scope for enhancement.

2. Related Work

Smart doorbell systems have gained significant attention in recent years, particularly with the increasing need for intelligent and secure access control mechanisms. Various researchers have proposed systems integrating biometric authentication, real-time communication, and IoT technologies to enhance residential and institutional security.
S. Pawar et al. proposed a face recognition-based smart doorbell system utilizing the OpenCV library on a Raspberry Pi platform [1]. Their approach focused on detecting and recognizing visitors using Haar-Cascade and LBPH classifiers. The system offered basic functionality but lacked real-time alerting mechanisms and remote control.

Another study by M. Khan et al. introduced an iris and voice recognition system to ensure privacy-focused home security [2]. This approach emphasized edge computing to protect biometric data by processing it locally. However, the implementation was limited in terms of scalability and intruder alerting features.

V. Bhanse and M.D. Jaybhaye developed a system combining ESP32-CAM modules with Wi-Fi integration for live video streaming to mobile devices when the doorbell is activated [3]. While effective in terms of visitor visualization, the absence of an intelligent classification model restricted its capability in intrusion detection scenarios.

In a more advanced system, D. R. Shenvi and K. Shet used deep learning models for facial recognition to automatically unlock the door when a known individual was identified [4]. Unknown visitors were notified to the user for manual verification. However, this system required constant internet connectivity and lacked support for emergency contact notifications and alarms.

Additionally, R. Lalitha et al. implemented an IoT-based surveillance system using a Raspberry Pi and motion detection sensors to trigger alerts during suspicious activity [5]. Although it provided basic intruder alert functionality, the system did not include any biometric verification or mobile interaction.

While the existing systems offer features such as video streaming, basic face recognition, or cloud integration, most of them are limited either by hardware capabilities, lack of dual-mode functionality, or insufficient real-time alerting and security controls. The proposed Bell Buddy system builds upon these works by integrating face recognition, real-time mobile alerts, motion sensing, and emergency contact notifications into a single, scalable platform suitable for modern smart homes.

3. System Design

The Bell Buddy Smart Doorbell System is designed as a dual-mode intelligent home security solution that seamlessly integrates image processing, IoT hardware, mobile applications, and cloud-based services. It operates under two modes: Doorbell Mode and Intruder Detection Mode, each triggered by specific user interactions or environmental cues. The system is built to ensure real-time monitoring, secure visitor verification, and timely alerts, all while maintaining a user-friendly experience.

3.1. Overall Architecture

The system consists of five major components:

1. ESP32 Microcontroller
   Responsible for handling the solenoid door lock, LED indicators, and communication between sensors and the cloud.
2. Raspberry Pi
   Functions as the processing unit for image capture and facial recognition. It runs the trained deep learning model for visitor verification.
3. HD Camera with Motion Sensor
   Mounted near the door, this module captures the visitor's image either upon bell press or motion detection.
4. Mobile Application (React Native)
   Serves as the user interface to receive visitor notifications, view images, manage access, and trigger alerts.
5. Firebase Cloud + PostgreSQL Database
   Firebase Cloud Messaging (FCM) is used for real-time notifications, while the PostgreSQL database stores registered user profiles, contacts, and image logs.

3.2. Modes of Operation

- Doorbell Mode
  When the doorbell is pressed, the system captures a real-time image using the HD camera and sends it to the user's mobile app. The user can verify the visitor and remotely trigger the solenoid lock to allow or deny access.
- Intruder Detection Mode
  The motion sensor detects activity near the door. If movement is detected, the system captures the individual's image and runs it through the facial recognition model. If the face is not matched with the authorized database, the system:
  - Sends alerts to the owner and emergency contacts
  - Activates a local alarm via the ESP32
  - Displays the intruder's image on the mobile app

3.3. Hardware Integration

The ESP32 is responsible for triggering the solenoid lock and managing status indicators. It receives signals via serial or Wi-Fi from the Raspberry Pi. The Raspberry Pi, programmed in Python, uses OpenCV and TensorFlow for facial recognition. The image is preprocessed before being compared with a dataset of known individuals stored in the database.

3.4. System Security

To ensure secure communication and data privacy:

- SSL (Secure Socket Layer) is used for encrypted communication between devices.
- JWT (JSON Web Token) authenticates users before allowing access to the app.
- AES (Advanced Encryption Standard) secures sensitive data like facial images and user credentials in the database.

3.5. Communication Workflow

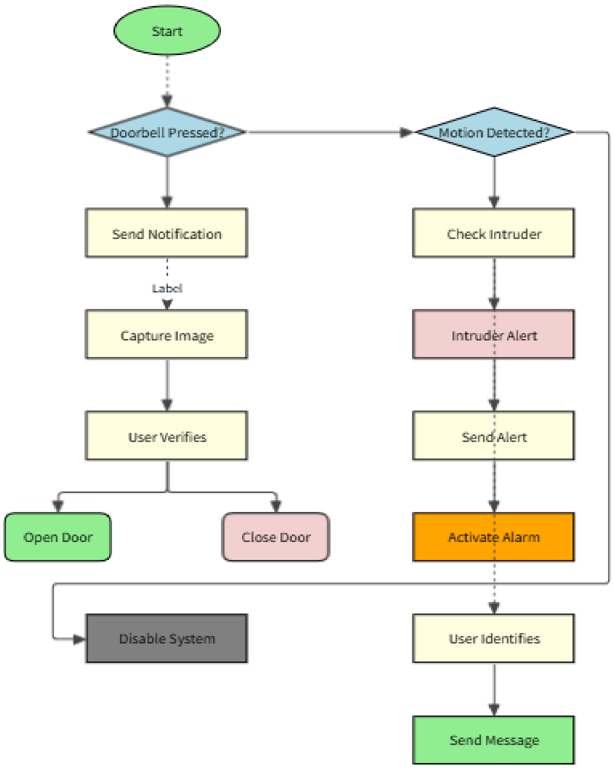
1. Doorbell or motion sensor triggers the system.
2. Image is captured and analyzed on Raspberry Pi.
3. Result is pushed to the mobile app using Firebase Cloud Messaging.
4. User makes a decision (unlock, ignore, alert).
5. System responds by unlocking door, activating alarm, or logging data.

4. Methodology

The proposed Bell Buddy Smart Doorbell System adopts a modular and layered approach to ensure secure, real-time visitor verification and automated intruder alerts. The methodology integrates IoT hardware, facial recognition algorithms, a mobile application, and real-time notification mechanisms.

4.1. System Workflow – Flowchart

The overall operation of the system can be summarized through the flowchart below:



4.2. Facial Recognition Algorithm

The facial recognition component is a critical aspect of the intruder detection mode. The following steps describe the algorithm:

- Face Detection:
  Uses Haar Cascade Classifiers from OpenCV to detect faces from the captured image in real-time.
- Preprocessing:
  The captured face image is resized, normalized, and converted to grayscale for faster processing.
- Feature Extraction:
  Local Binary Pattern Histogram (LBPH) is applied to extract unique features from the detected face.
- Classification:
  A pre-trained Convolutional Neural Network (CNN) model using TensorFlow/Keras is used to classify the face as known or unknown.
- Thresholding Decision**:**
  If the confidence score from the model is above a certain threshold (e.g., 80%), the person is marked as "Authorized." Otherwise, an alert is triggered.

4.3. Motion Detection System

A PIR (Passive Infrared) sensor is used to detect movement in front of the door. When motion is detected:

- The Raspberry Pi activates the camera module.
- An image is captured for analysis.
- Facial recognition is run immediately, even if the doorbell is not pressed.

This enables proactive surveillance and threat detection.

4.4. Mobile App Control Interface

The user interacts with the system through a React Native-based mobile app that supports:

- Login and secure access (using JWT authentication).
- Viewing real-time visitor images.
- Unlocking the door remotely (via ESP32 command).
- Receiving intruder alerts via Firebase Cloud Messaging (FCM)**.**
- Notifying emergency contacts with one-tap messaging.

4.5. Solenoid Lock Control via ESP32

The ESP32 microcontroller acts as the hardware gateway for door access:

- Receives unlock/lock signals from the app or Raspberry Pi.
- Activates the solenoid lock based on verification.
- Controls buzzer for intruder alerts and LEDs for status indicators.

The ESP32 communicates with Firebase and the Raspberry Pi via Wi-Fi.

4.6. Backend Database and Security

- All user data, contact information, and logs are stored in a PostgreSQL database.
- Drizzle ORM is used for efficient backend interaction.
- AES encryption secures sensitive data.
- Communication between modules is protected using SSL**.**

5. Results and Discussion

This section evaluates the performance of the **Bell Buddy Smart Doorbell System** based on its facial recognition accuracy, system responsiveness, and reliability in both operational modes. The experimental setup uses a Raspberry

Pi for processing and an ESP32 microcontroller for hardware control. The facial recognition model was trained and validated over 50 epochs using a dataset of authorized and unauthorized faces.

5.1. Model Accuracy

The system achieved high classification accuracy in recognizing known and unknown individuals. The model showed progressive improvement in both training and validation accuracy with each epoch.

Table 1. Accuracy and Validation Accuracy across Epochs

Epochs	Accuracy (%)	Valid Accuracy(%)
1	60	58
5	72	70
10	80	78
15	85	83
20	88	86
25	90	88
30	91	89
35	92	90
40	93	91
45	94	92
50	95	3

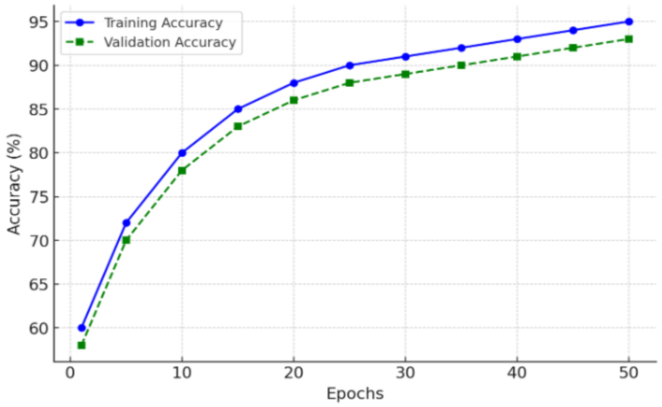


Figure 1. Accuracy Plot Over Epochs

5.2. Model Loss

The loss function steadily decreased during training, indicating proper model convergence.

Table 2. Training and Validation Loss over Epochs

Epoch	*Training Loss*	*Validation Loss*
1	*0.872*	*0.940*
2	*0.677*	*0.769*
3	*0.520*	*0.609*
4	*0.499*	*0.559*
5	*0.369*	*0.455*
6	*0.267*	*0.416*
7	*0.244*	*0.342*
8	*0.169*	*0.292*
9	*0.158*	*0.263*
10	*0.157*	*0.258*
11	*0.082*	*0.251*
12	*0.105*	*0.152*

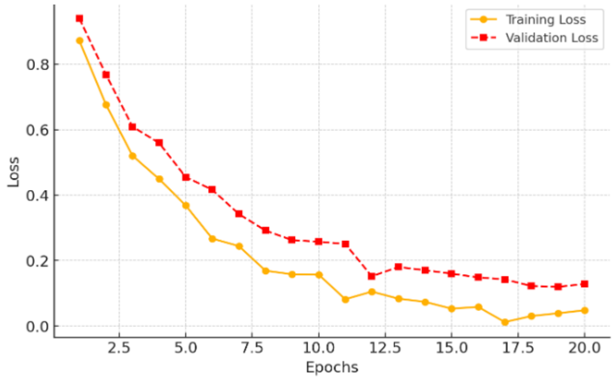


Figure 2. Loss Plot Over Epochs

5.3. Classification Performance

The performance of the facial recognition classifier is measured using precision, recall, and F1-score metrics.

Table 3. Classification Report

Class	**Precision**	**Recall**	**F1-Score**	**Support**
Intruder	0.875	0.778	0.824	9
Authorized	0.833	0.909	0.870	11
Overall Accuracy	-	-	**0.85**	20

These results show the model performs reliably in distinguishing between authorized and unauthorized individuals, with an overall accuracy of **85%**.

5.4. Confusion Matrix

The confusion matrix visually represents correct and incorrect classifications.

Figure 3. Confusion Matrix

	Predicted Intruder	**Predicted Authorized**
Actual Intruder	7	2
Actual Authorized	1	10

5.5. Violin Plot – Accuracy Distribution

A violin plot is used to show the distribution of accuracy across epochs, combining a box plot with a density trace.

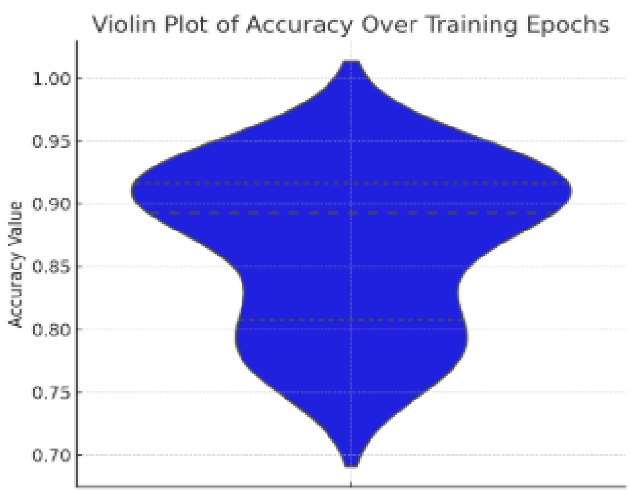


Figure 4. Violin Plot of Accuracy Distribution

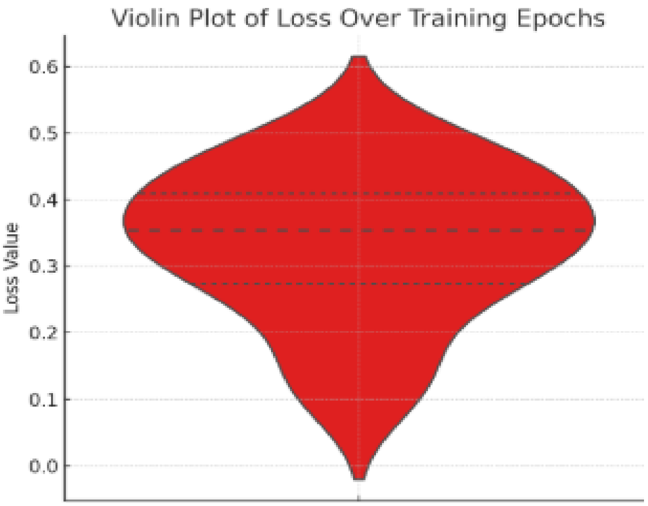


Figure 5. Violin Plot of Loss Distribution

5.6. Comparative Analysis
To benchmark performance, Table 4 compares **Bell Buddy** with two existing systems.

Table 4. Comparative Performance Analysis

Feature/Metric	Proposed System	System A [1]	System B [2]
Facial Recognition	☑ Yes	☑ Yes	✕ No
Mobile Notification	☑ Yes	✕ No	☑ Yes
Intruder Alert	☑ Yes	✕ No	☑ Limited
Emergency Contact Alert	☑ Yes	✕ No	✕ No
Recognition Accuracy	85%	72%	65%
Alarm/Buzzer Integration	☑ Yes	✕ No	☑ Yes

This comparison shows that **Bell Buddy** offers a more complete and responsive system for home security, outperforming prior approaches in terms of both features and accuracy.

6. Conclusion and Future Scope

The development of the Bell Buddy Smart Doorbell System presents an effective, low-cost, and intelligent solution for enhancing home and institutional security. By combining the capabilities of IoT devices, facial recognition technology, and real-time mobile notifications, the system offers a dual-mode operating mechanism that improves safety and user convenience. The Doorbell Mode facilitates secure visitor verification by sending real-time images to the user's mobile application, allowing them to control access remotely. In contrast, the Intruder Detection Mode actively monitors suspicious activity using a motion sensor and classifies individuals through a facial recognition model. The system achieved 85% classification accuracy, indicating promising real-world usability. The integration of hardware components such as ESP32, Raspberry Pi, and PIR sensors, along with cloud support from Firebase, contributes to seamless and secure system operation. The inclusion of emergency contact alerts, solenoid lock activation, and user-friendly mobile interface makes the system scalable for deployment in homes, offices, hostels, and other entry-controlled environments.

Despite its success, the system has limitations such as reduced facial recognition accuracy in low-light environments and dependency on uninterrupted network connectivity for real-time operation. The accuracy and response speed may also be influenced by variations in camera angle, face orientation, and distance from the lens. These constraints may affect the system's performance in highly variable conditions.

In future work, the system can be expanded to support voice command control through integration with AI assistants like Alexa or Google Assistant. Cloud-based face recognition APIs can be incorporated for faster and more scalable processing. Enhancements such as night vision cameras, biometric sensors, or QR code access can be introduced for improved versatility. Long-term data logging and analytics features could also enable behavioral pattern detection for high-security areas. These advancements will ensure the Bell Buddy system evolves into a comprehensive smart access control solution suitable for both personal and commercial security needs.

Authors' Contributions
Sivakami T S conceptualized the project, led the mobile app development, and managed system integration. Alphia Jose handled the ESP32 programming and solenoid lock control. Hredya Vijay worked on image processing and camera module integration. Jasmin Maria Binoy performed literature review, compiled documentation, and structured the manuscript. All authors reviewed and approved the final version of the manuscript.

Acknowledgements
The authors would like to thank the Department of Computer Science and Engineering, AISAT, for their support, mentorship, and the facilities provided throughout the completion of this project. Special thanks to our project guide, Angel Mathai, for her invaluable insights and encouragement.

References

[1] S. K. Sharma, L. Gupta, "A Novel Approach for Cloud Computing Environment," *International Journal of Computer Sciences and Engineering*, Vol.4, Issue.12, pp.1-5, 2014.
[2] M. Khan, H. Anum, S. Batool, B. Bashir, "Smart Home with Wireless Smart Doorbell with Smart Response," *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Turkey, pp.120–124, 2021.
[3] S. Pawar, V. Kithani, S. Ahuja, S. Sahu, "Smart Home Security using IoT and Face Recognition," *2018 International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, pp.1–5, 2018.
[4] V. Bhanse, M. D. Jaybhaye, "Face Detection and Tracking using Image Processing on Raspberry Pi," *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, India, pp.542–545, 2018.

[5] D. R. Shenvi, K. Shet, "CNN Based Face Recognition for Home Security," *International Conference on AI and Smart Systems (ICAIS)*, India, pp.873–878, 2021.
[6] R. V. S. Lalitha, K. Kavitha, N. V. Krishna Rao, "Smart Surveillance with Smart Doorbell," *IEEE Access*, Vol.8, pp.118309–118321, 2020.
[7] A. Mardin, T. Anwar, B. Anwer, "Image Compression using Discrete Transformation and Matrix Reduction," *International Journal of Scientific Research in Biological Sciences*, Vol.5, No.1, pp.1–6, 2017.
[8] H. R. Singh, "Randomly Generated Algorithms and Dynamic Connections," *International Journal of Scientific Research in Biological Sciences*, Vol.2, Issue.1, pp.231–238, 2014.
[9] C. Todeka, "Principle of Data Securing," *IJCSE Publication*, India, pp.03–05, 2022.
[10] S. T. Tanwar, "Dive in Market of Crypto Currencies," *Journal of Computer Science and Engineering*, Vol.13, Issue.1, pp.12–20, 2024.

AUTHORS PROFILE

Sivakami T S is currently pursuing B.Tech in Computer Science and Engineering at Albertian Institute of Science and Technology (AISAT), Kerala and is affiliated to APJ Abdul Kalam Technical University. She conceptualized the Bell Buddy project, led the development of the mobile application, and managed overall system integration. Her interests include full-stack development, embedded systems, and innovative IoT solutions.

Jasmin Maria Binoy is currently pursuing B.Tech in Computer Science and Engineering at Albertian Institute of Science and Technology (AISAT), Kerala and is affiliated to APJ Abdul Kalam Technical University. She contributed to the documentation, related work analysis, and formatting of the Bell Buddy project. Her areas of interest include technical communication, software documentation, and research support. She is also passionate about artificial intelligence, smart security systems, and project management.

Alphia Jose is currently pursuing B.Tech in Computer Science and Engineering at Albertian Institute of Science and Technology (AISAT), Kerala and is affiliated to APJ Abdul Kalam Technical University. She handled the ESP32 programming and solenoid lock control for the Bell Buddy system. Her interests include IoT systems, hardware-software integration, embedded development, and mobile applications.

Hredya Vijay is currently pursuing B.Tech in Computer Science and Engineering at Albertian Institute of Science and Technology (AISAT), Kerala and is affiliated to APJ Abdul Kalam Technical University. As a key contributor to the Bell Buddy project, she worked extensively on the image processing pipeline and camera module integration, ensuring seamless visual data capture and real-time analysis. Her interests include artificial intelligence, smart security systems, and real-time automation.

