Smart Door Unlock System with Android App

Jeenat Sultana
Computer Science Department
Southern University Bangladesh
Chttagong, Bangladesh
jeenatcse@gmail.com

Shusmoy Chowdhury
Computer Science Department
Missouri State University
Springfield, Missouri, USA
shusmoy26@missouristate.edu

Moynul Hasan Tushar
Computer Science Department
Southern University Bangladesh
Chttagong, Bangladesh
tmoynulhasan@gmail.com

Md.Hemayet Uddin
Computer Science Department
Southern University Bangladesh
Chttagong, Bangladesh
uhemayet9@gmail.com

2024 IEEE Region 10 Symposium (TENSYMP) | 979-8-3503-6486-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/TENSYMP61132.2024.10752104

***Abstract*—The security of a room hinges on effective locking mechanisms, particularly when unauthorized access is rigorously prevented. Various methods, such as face detection, voice and speech recognition, password and PIN codes, and biometric technologies, serve as digital keys for door locking and unlocking. With the proliferation of Android devices, these digital keys are increasingly integrated into Android applications. In this research, we present a system designed to achieve two primary objectives. First, ensuring authorization by preventing unauthorized access to secured rooms. Second, facilitating the transfer of authorization to an unauthorized individual in emergency situations. To achieve the first objective, we employed face detection and speech recognition technologies, while for the second, we utilized random one-time passwords. Both functionalities were implemented through Android applications and interfaced with an Arduino Nano via a Bluetooth module. Additional security measures were incorporated using sensors to detect forceful intruder attacks. Our research objective was to devise a system that combines enhanced security measures with cost-effectiveness. Based on the analysis of the results, it is evident that the proposed low-cost solution has demonstrated satisfactory performance, achieving a 98% accuracy rate in securing the home locking system. Consequently, this solution has proven to be both affordable and practical for real-world applications.**

***Index Terms*—Android App, Arduino Nano, Face Detection, IoT, Speech Recognition.**

I. Introduction

Researchers are diligently endeavoring to guarantee the security and safety of our lives and residences. Nevertheless, concerns regarding security are escalating swiftly. Property crime constitutes over 85% of all crime in the US as of 2021, with reported stolen property worth over 737 billion USD, of which approximately 12% was recovered [1]. Consequently, it has emerged as an urgent global requirement [2]. To meet this exigency, researchers have conceived and crafted various locking systems aimed at ensuring the security of properties and residences.

The evolution of locking systems has become pivotal in bolstering the security infrastructure of residential premises. The imperative of securing our homes during periods of absence necessitates robust mechanisms. Traditional lock and key setups have long served this purpose. However, with the advent of scientific and technological advancements, novel lock designs have emerged, aimed at fortifying residences against unwarranted intrusions. Concurrently, the ubiquitous nature of mobile phones in contemporary lifestyles presents an opportunity to integrate security systems seamlessly with mobile devices, offering heightened effectiveness and convenience.

In the contemporary era, residential automation extends from the very threshold, encompassing tasks such as door unlocking and management of household appliances. Leveraging Android devices as automated controllers not only fulfills the demand for digital keys but also leverages the high-resolution cameras embedded in these devices, obviating the need for external closed-circuit cameras. Furthermore, the integration of facial recognition features within mobile cameras has become a standard application. Considering these advancements, our project's focal point is securing access to private spaces within homes.

This endeavor is part of a broader home automation framework [3] and serves as a demonstrative instance of the Internet of Things (IoT) [4]. Employing a multi-layered security approach, our system facilitates two distinct user access levels. Authorized users, equipped with the designated smartphone app, undergo a process involving facial detection and security question verification. Alternatively, temporary users can request and receive a one-time password (OTP) through the app for limited access. Facial recognition employs the Principal Component Analysis (PCA) algorithm [5]–[7], a widely adopted technique for this purpose. Furthermore, utilizing smartphones as keys mitigates the risk of forgetting physical keys.

The remainder of this paper is structured as follows: Section II delves into related research conducted by various scholars in this domain. Section III outlines our project's methodology, subdivided into System Design and Hardware Components. Section IV elaborates the system implementation of our research. Section V presents an analysis of outcomes derived

979-8-3503-6486-6/24/$31.00 ©2024 IEEE

from our project, while Section VI encapsulates conclusive remarks. Our project's overarching goal is to devise a smart unlock system seamlessly integrated with an Android application, enhancing the security paradigm of residential spaces.

II. Related Work

Now-a-days our home is getting automated from the very entrance with unlocking a door to the handling of home appliances [8], [9]. The use of android devices as automated controllers meets not only the need of digital keys but also the high resolution mobile camera replaces the need of external closed circuit camera. Moreover, tagging the recognized faces in an image is now an in-built application of the mobile camera. Bearing in mind all these facilities we, in our project, focused on the secure entrance to a private room.

Vanita Jain et al. [10] designed and developed an autonomous video surveillance system that is proficient in detecting, identifying, and tracking individuals within a video stream.The approach utilizes the computationally efficient and accurate object tracker, Deep SORT, in conjunction with the highly precise but computationally intensive facial recognition model, FaceNet. The proposed method results in a 115% increase in runtime due to the integration of these two components.

M Shanthini et al. [11] designed a door locked system through a smartphone-controlled, Bluetooth-connected mechanism utilizing the Arduino UNO platform for enhancement security by enabling building owners to monitor and control access. The system allows users to remotely operate the door lock via a specially developed Android application, compatible with devices such as tablets, smartphones, and laptops. Access is granted upon successful verification of login credentials (username and password), which are authenticated against a database over the internet. In the event of invalid credentials, a buzzer is activated, and an SMS alert is immediately dispatched to the building owner, thereby reinforcing security measure

Renu Dalal et al. [12] has used biometric authentication for user classification in metro rail ticket management in india. The paper proposes a novel ticketing system for metro passengers utilizing facial recognition technology. It outlines the implementation process of this system and demonstrates how passengers can effectively manage their metro accounts using the proposed technology.

Kartik A Patil et al. [13] designed a device using an Arduino Nano that offers physical security by using the biometric sensor found in smartphones. Fingerprint technology is highly accurate and cost-effective. It is almost impossible to duplicate, with only a one in a billion chance of it being copied. Biometric security provides a reliable way to identify users using something that can't be lost, copied, or stolen. The proposed system is affordable, easy to set up, and works in different ways, making it very useful.

Anjali Patel et al. [14] introduced an idea of secure door locking system using Raspberry pi (RPi) server system to control the video camera for capturing images on a relay and unlock the door comparing the image of the user with the images in database. Using Raspberry pi server system possess a secure system with high expense, not easily affordable by an individual.

Vamsi, T. K., et al. [15] proposed a real-time face recognition system for door unlocking using LBPH algorithm. The algorithm was used to convert the color image to a pixel matrix format before storing to the database. The pixel values in the matrix are compared to the pixel values of the user's image for detecting his or her face. Retha Dinar Hayu Arifin et al. [16] designed a system where the door is unlocked using speech command or pincode and the speech command or pincode is given via smart phone.

Agbo David et al. [17] implemented a system of door unlocking using password via Android App. Abdul Azeemet al. [18] implemented face recognition for door unlocking using the viola jones method for face detection and the Local Binary Patterns Histograms for face recognition. Patel, P.et al. [19] proposed and implemented the door locking and unlocking system with smart phones using wi-fi connectivity. Every of the above mentioned researches ensures high security but encompasses components that are lavish and needs experts to design.

In our paper we proposed and implemented a cost-effective door unlock system using face detection and speech recognition via Android app. Along with the system we added the facility of requesting for a password, an alarm system in case of intruder attack and a LCD display to interpret the progress of work. We designed our system economically and kept it simple so that not only an official but also an ordinary being can bear the expenses and use the system for securing his own room.

III. Methodology

The methodology employed in this study is delineated through three key components: system design, hardware elements, and system implementation. The system design section provides a comprehensive overview of the system's intricacies, encompassing flow charts, block diagrams, and circuit diagrams to elucidate its operational framework. Additionally, the hardware components section furnishes a detailed exposition of the physical components utilized in realizing the design blueprint. Finally, the system implementation segment encapsulates the actualization of the designed system, detailing its functional manifestation.

User categorization forms a pivotal aspect of this study, delineating distinct pathways of access. The 'legitimate owner' pertains to the individual who holds ownership rights over the system. On the other hand, an 'authorized user' signifies an individual or a group granted explicit authorization by the legitimate owner to unlock the system. Conversely, an 'unauthorized user' typically lacks inherent access privileges but may be granted temporary access by the legitimate owner as needed.

A. System Design

The system design encompasses two distinct methods of access, delineated in the flowchart depicted in “Fig 1”. These methods, labeled as ’Authorization Check’ and ’Authorization Provided,’ cater to different user scenarios and security protocols.

The ’Authorization Check’ process pertains to individuals already registered in the system as authorized users. To ensure secure access, a dual-layer security mechanism has been implemented, leveraging facial detection and speech recognition. This multi-layered security protocol is embedded within an Android application, which interfaces with the microcontroller unit ”Arduino Nano” through a Bluetooth module.

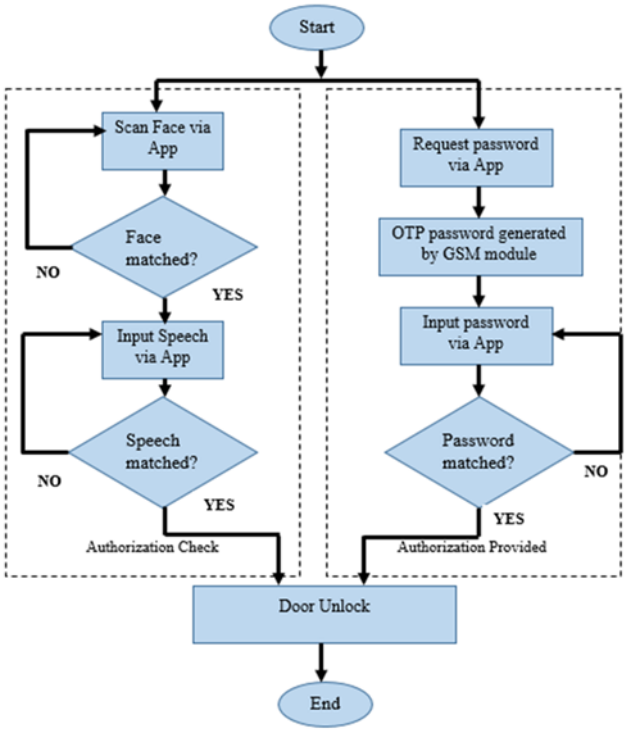

Fig. 1. Flow Chart of the System

Authorized users, whose facial profiles are pre-scanned and stored in the system’s database, initiate the unlocking process by scanning their faces using the mobile app’s camera, as illustrated in “Fig 1”. Upon successful facial recognition, they proceed to the second security layer, which involves speech recognition through a series of predefined security questions. The system employs three such questions, requiring accurate responses to each for successful authentication. These security questions can be periodically modified for enhanced security based onowner’s specifications. Users initiate the security question process by utilizing the ’ask’ button within the Android app, verbally responding to the questions for speech recognition verification. The sequential implementation of face and speech recognition layers ensures stringent access control; failure to pass either layer maintains the door’s locked status.

The ’Authorization Provided’ method supplements the system by granting temporary access to unauthorized users. In this scenario, individuals lacking prior authorization but requiring access can request a OTP through the app. The request triggers the ’Arduino Nano’ to generate a random OTP via the GSM module, which is then relayed to the legitimate owner for dissemination. Upon inputting the correct OTP, the unauthorized user gains short-term access.

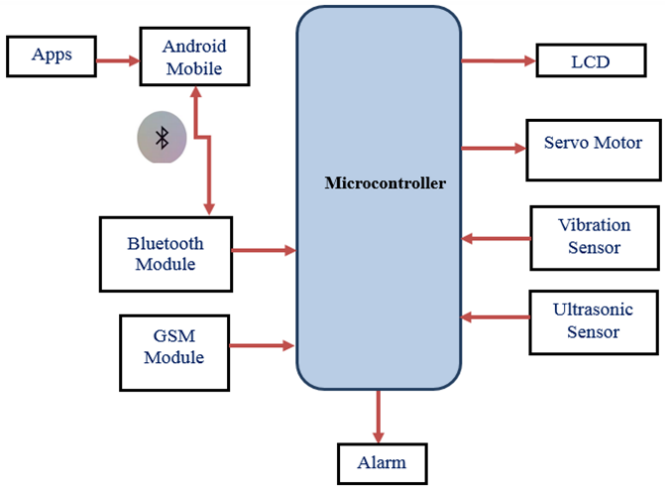

Fig. 2. Block Diagram of the System

The system’s hardware components, illustrated in “Fig 2”, comprise various sensors interfaced with the Arduino Nano. Researchers has been continuously using these components to design effective IoT systems [20]. These include a vibration sensor and an ultrasonic sensor, tasked with detecting unauthorized attempts to force open the door. Upon detection of such intrusion attempts, an alarm is activated, and an alert message is dispatched to the authorized user via the GSM module. Additionally, an LCD display module provides real-time system status updates, facilitating monitoring and oversight.

The operational framework of the system spans three primary phases: database creation and user registration, image scanning and comparison for access control, and intruder reporting and network-enabled owner intervention. This systematic approach ensures robust security measures and responsive action capabilities.

B. Hardware Components

The list of hardware components employed in the circuit shown in “Fig 3” are elaborated below:

1) Arduino Nano: Arduino Nano is the main controlling unit to which other modules and sensors are connected [18]. It is a microcontroller board designed by Arduino.cc. The microcontroller used in the Arduino Nano is Atmega328, the same one as used in Arduino UNO. It is a microcontroller board well-known for its small size and flexibility and possess a wide range of application areas. Initially, we captured the images of the authenticated users to create a database for

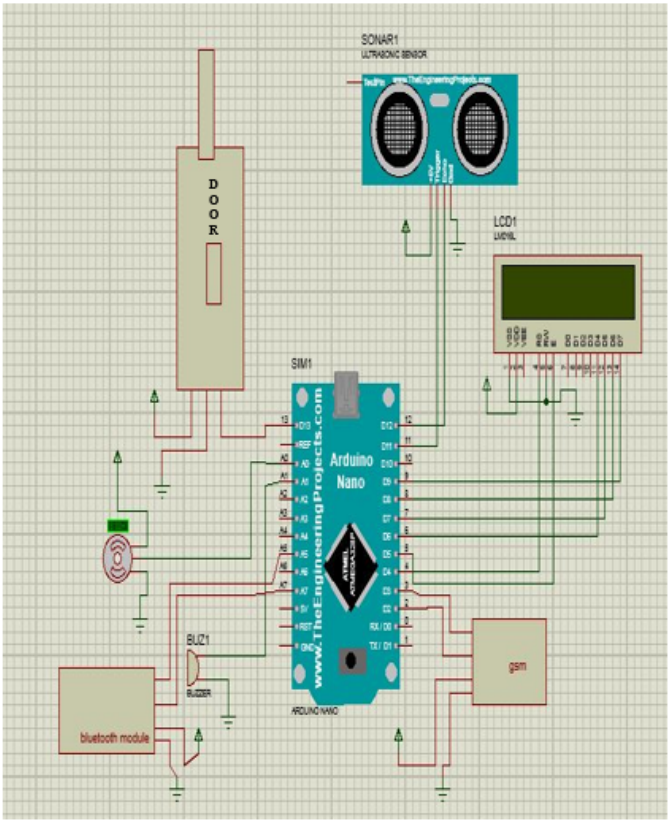

Fig. 3. Circuit Diagram

Arduino Nano module storage system and this database is compared to the live image captured and provided by the camera module of android device. After comparing two images using PCA algorithm [7], [21], output is considered to be positive/negative as this controller is digital; and based on the output response, it gives commands to GSM module.

2) Vibration Sensor: Vibration sensors, also known as piezoelectric sensors, are versatile tools for the measurement of various processes. These sensors use the piezoelectric effect, which measure changes in pressure, acceleration, temperature, strain or force by converting them to an electrical charge. The vibration sensor is used in the system to detect any kind of unethical access when an intruder wants to break the door.

3) Ultrasonic Sensor: The HC-SR04 ultrasonic sensor uses sonar to determine distance to an object like the way bats do. It offers excellent non-contact range detection with high accuracy and stable readings in an easy-to-use package. It comes in complete with ultrasonic transmitter and receiver module. It provides 2cm - 400cm non-contact measurement function. In our system, this sensor works simultaneously with the vibration sensor to detect attack.

4) Bluetooth Module: The version of Bluetooth module we used in our system is the HC-05 module. It has a default Baud rate of 38400. The android app gets the connectivity with the Arduino Nano via this module.

5) GSM Module : GSM is an open and digital cellular technology used for transmitting mobile voice and data services. A GSM digitizes and reduces the data, then sends it down through a channel with two different streams of client data, each in its own particular time slot. SIM800L GSM/GPRS module is a cheap miniature GSM modem that is used for IoT projects. In our system, GSM module is used for sending a message to the authorities after comparing the captured image with the stored images and based on whether the output is positive or negative. If the output comes out positive it means the person is identified and the door is unlocked.

6) Servo Motor: The servo motor is commonly used for automation technology in the industrial application areas. It is a self-contained electrical device that can rotate parts of a machine with high efficiency and great perfection. The output shaft of this motor can be moved to a particular angle. We used the servo motor to unlock the door.

IV. System Implementation

The system implementation involved a meticulous approach across two distinct domains: hardware development and software application design. Firstly, we devised the hardware module, as delineated in the block diagram and circuit diagram showcased in Figures 2 and 3, respectively. Concurrently, we engineered the Android application, visualized through the flowchart in "Fig 1". The integrated circuit, as illustrated in "Fig 4", forms the nexus of connectivity between the designed app, showcased in "Fig 5", and the hardware components, facilitated via a Bluetooth module.

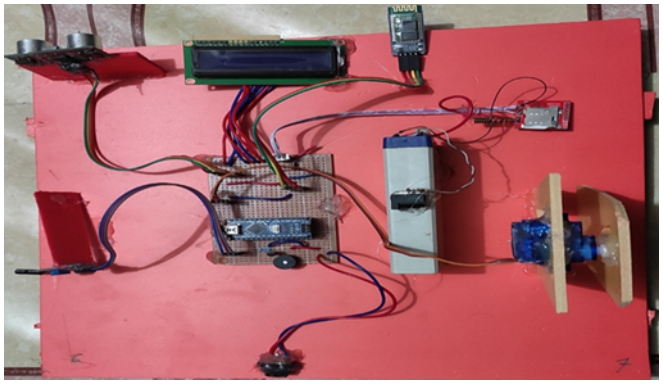

Fig. 4. Project Circuit View.

The Android application assumes a pivotal role in facilitating facial and speech recognition functionalities. Developed using Android Studio, the application harnesses the power of the PCA algorithm for robust facial detection and recognition within images. This algorithmic implementation within the app ensures precise identification of authorized users, aligning with the system's security protocols.

The hardware module encompasses a sophisticated architecture, meticulously designed to synchronize with the Android application seamlessly. The block diagram and circuit diagram, depicted in Figures 2 and 3, respectively, delineate the intricate interplay of components such as sensors, microcontrollers,

and communication modules. These components work synergistically to enable functionalities like intrusion detection, system monitoring, and communication with the Android app via Bluetooth connectivity.

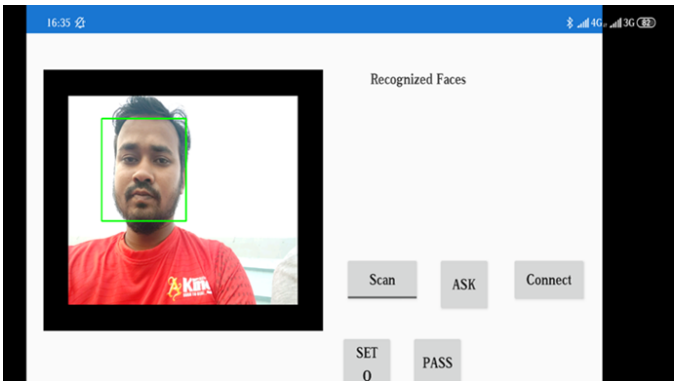

Fig. 5. Android App View

The culmination of these efforts is the synchronized operation between the Android application and the hardware module. The app's capabilities for facial and speech recognition are seamlessly integrated with the hardware's sensor-driven functionalities. This cohesive integration ensures a robust and comprehensive security system, capable of detecting intrusions, authenticating authorized users, and facilitating secure access to designated spaces. The systematic implementation across hardware and software domains underscores the sophistication and reliability of the developed system, aligning with contemporary standards of smart security solutions.

V. Results and Analaysis

The system underwent rigorous testing to evaluate its efficacy across multiple security phases, encompassing both authorized and unauthorized access scenarios. In the initial phase, verification of authorized users involved a sample set of approximately 20 faces. Upon facial detection, users were subjected to three security questions as per protocol. The resulting data were classified and cataloged, as detailed in Table I, showcasing the system's performance metrics.

Concurrently, the system's capacity to grant authority to unauthorized users was evaluated. Leveraging passwords for this purpose, the system demonstrated its adaptability and network portability. Unauthorized users, lacking facial database entries, could request passwords via the app. The generated password, relayed through the GSM module to authorized personnel, enabled temporary access upon successful validation. This process, outlined in Table II, illustrates the system's robustness in managing diverse access scenarios.

The system's performance was meticulously assessed, culminating in a remarkable accuracy rate of 98% for the authorization checking phase and an impeccable 100% accuracy in the authorization provisioning phase. These results underscore the system's reliability and effectiveness in maintaining stringent security protocols.

TABLE I
Result Testing For Authorization Check

Sl No	Face check	Question	Serial Number	Face check
1	OK	OK	Open	OK
2	Wrong	OK	Close	OK
3	OK	Wrong	Close	OK
4	Wrong	Wrong	Close	OK

TABLE II
Result Testing For Providing Authorization

Sl No	Request for OTP	Input OTP	Door condition	System
1	OK	OK	Open	OK
2	OK	Wrong	Close	OK

Moreover, a critical aspect of our research focused on economic viability. The cost analysis, delineated in Table III, demonstrates the system's cost-effectiveness, with a hardware expenditure of BDT 1695. This economical investment aligns with our objective of designing a system that is both efficient and financially accessible.

TABLE III
Cost Calculation

Serial Number	Components name	Cost(in BDT)
1	Vibration sensor	80
2	Bluetooth sensor (Hc05)	260
3	Ultrasonic sensor	80
4	LCD	110
5	Vero board	20
6	Buzzer	10
7	Arduino Nano	60
8	Power Supply (SMPS)	80
9	GSM Module (SIM 800L)	450
10	Servo Motor	150
11	Battery	95
12	Others	200
	Total Cost	1695

In essence, the comprehensive testing and analysis reaffirm the system's proficiency in safeguarding access to designated spaces, while also emphasizing its affordability and practicality in real-world applications.

VI. Conclusion

In conclusion, our research culminated in the development of a system aimed at enhancing security with minimal human intervention and affordable costs. The system's simplicity, affordability, and reliability make it an accessible solution, with readily available hardware components and easy portability and upgradability. By targeting the security of a single room with limited authorized access, we optimized internal storage requirements, thereby reducing costs.

An effective alarm and notification system were integrated for timely intrusion detection, allowing valid users to promptly address any security breaches. While our focus was on securing a specific room in a cost-effective manner, future enhancements could involve scaling up to larger environments such as entire homes or offices. In such scenarios, utilizing

Firebase as an extended database could accommodate a larger user base.

Furthermore, considering future prospects, incorporating a closed-circuit camera system with Raspberry Pi could enhance computational capabilities and provide more robust security measures. These potential developments align with our research's overarching goal of continually improving security systems while maintaining affordability and efficiency. In the future, we plan to integrate machine learning techniques to analyze user patterns related to locking and unlocking behaviors. This will enable the automated locking of homes based on detected user routines and provide notifications in the event of unauthorized intrusions.

REFERENCES

[1] F. USA, "Crime data explorer," 2022. [Online]. Available: https://cde.ucr.cjis.gov/LATEST/webapp/pages/explorer/crime/crime-trend

[2] R. Edwards, "The state of safety in america 2023," Aug 2023. [Online]. Available: https://www.safewise.com/state-of-safety/

[3] G. Panwar, R. Maurya, R. Rawat, R. Kanswal, and P. Ranjan, "Home automation using iot application," *International Journal of Smart Home*, vol. 11, no. 9, pp. 1–8, 2017.

[4] V. Sharma and R. Tiwari, "A review paper on "iot" & it's smart applications," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 5, no. 2, pp. 472–476, 2016.

[5] K. R. Pattipati and J. L. Wolf, "A file assignment problem model for extended local area network environments," in *Proceedings., 10th International Conference on Distributed Computing Systems*. IEEE Computer Society, 1990, pp. 554–555.

[6] J. Williams, "Narrow-band analyzer," phd dissertaion," *Department of Electrical Engineering, Harvard University, Cambridge, MA*, 1993.

[7] A. Vinay, C. A. Kumar, G. R. Shenoy, K. B. Murthy, and S. Natarajan, "Orb-pca based feature extraction technique for face recognition," *Procedia Computer Science*, vol. 58, pp. 614–621, 2015.

[8] U. Sugandh, S. Nigam, and M. Khari, "Integrated approach using blockchain, sensors and smart contracts for weather alert," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2024, pp. 1699–1705.

[9] J. M. Chatterjee, R. Kumar, M. Khari, D. T. Hung, and D.-N. Le, "Internet of things based system for smart kitchen," *International Journal of Engineering and Manufacturing*, vol. 8, no. 4, p. 29, 2018.

[10] V. Jain, M. S. Pillai, L. Chandra, R. Kumar, M. Khari, and A. Jain, "Camaspect: an intelligent automated real-time surveillance system with smartphone indexing," *IEEE Sensors Letters*, vol. 4, no. 10, pp. 1–4, 2020.

[11] M. Shanthini, G. Vidya, and R. Arun, "Iot enhanced smart door locking system," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, 2020, pp. 92–96.

[12] R. Dalal, M. Khari, M. N. Arbab, H. Maheshwari, and A. Barnwal, "Smart metro ticket management by using biometric," in *Multimodal Biometric Systems*. CRC Press, 2021, pp. 101–110.

[13] K. A. Patil, N. Vittalkar, P. Hiremath, and M. A. Murthy, "Smart door locking system using iot," *International Research Journal on EngTechnol (IRJET)*, pp. 3090–3094, 2020.

[14] A. Patel and A. Verma, "Iot based facial recognition door access control home security system," *International Journal of Computer Applications*, vol. 172, no. 7, pp. 11–17, 2017.

[15] T. Vamsi, K. C. Sai, and M. Vijayalakshmi, "Face recognition based door unlocking system using raspberry pi," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 5, no. 2, pp. 1320–1324, 2019.

[16] R. D. H. Arifin and R. Sarno, "Door automation system based on speech command and pin using android smartphone," in *2018 International Conference on Information and Communications Technology (ICOIACT)*. IEEE, 2018, pp. 667–672.

[17] O. A. David, M. Chinaza, and O. Jotham, "Design and implementation of a door locking system using android app," *Int. J. Sci. Technol. Res*, vol. 6, no. 08, pp. 198–203, 2017.

[18] A. Azeem, S. Rao, K. Rao, S. Basha, H. Pedarla, and M. Gopi, "Door unlock using face recognition," *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, vol. 6, no. 4, pp. 240–243, 2017.

[19] P. Patel and S. Ajani, "The digital locking and unlocking system based on android for smart phone," *International Journal*, vol. 6, no. 2, 2016.

[20] L. Louis, "working principle of arduino and u sing it," *International Journal of Control, Automation, Communication and Systems (IJCACS)*, vol. 1, no. 2, pp. 21–29, 2016.

[21] H. Makwana and T. Singh, "Comparison of different algorithm for face recognition," *Global Journal of Computer Science and Technology Graphics & Vision*, vol. 13, no. 9, 2013.