International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03372
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Secure Your Entry Ways: Using Cloud Based Door Access System

Miss. Jayshree Rajendra Sanap[1], Mr. Aditya Sharad Sanap[2], Mr. Omkar Dnyaneshwar Dighole[3], Miss. Neha Kishor Salve[4], Prof. Bharti M. Gawale[5].

[1,2,3,4,5] Department of Computer Engineering, Loknete Gopinathji Munde Institute of Engineering Education and Research, Nashik, India.

Abstract - In this paper, we emphasize the protection of entry points through a cloud-based door access system based on our earlier conceptual design to provide a fully developed prototype. Meeting today's security demands, the system takes advantage of IoT technology for effective visitor tracking and access control in residential and commercial buildings. The model deployed employs a Raspberry Pi as the processing unit, coupled with a Pi camera that takes real-time photographs of visitors when the doorbell is pressed. The photographs are sent in real-time to a Dropbox cloud server, where they are stored securely encrypted, providing tamper-proof digital records for future authentication [3]. The system increases post-conflict security by being able to keep log records of current activities, which can be presented electronically in times of conflict or incidents. Managed through a mobile app, authorized personnel are able to control visitor access remotely, receiving real-time alerts and images to make the decision whether to grant entry. This ensures safe and verified access control. Cloud integration offers scalability and remote management across numerous properties through a single platform [2]. The deployed prototype, which was put to the test in a simulated setting, boasts high reliability, with 97% accuracy in fingerprint authentication and a response time of 2 seconds. This "Secure Your Entry Ways: Using Cloud-Based Door Access System" integrates IoT technology, mobile app control, and safe cloud storage to present a dependable, effective solution for contemporary security requirements, real-time monitoring, safe record-keeping, and distant management, improved user convenience and security.

***Key Words*:** IOT, Door Lock, Cloud Computing Security, Biometric Authentication, Fingerprint Sensor, Raspberry Pi.

1.INTRODUCTION

This paper, "Secure Your Entry Ways: Using Cloud-Based Door Access System," develops our previous conceptual project to a totally finished and tested model, which is a game-changer for conventional door and access control in contemporary security. From the combination of a smart door lock system with IoT technology, biometric identification, cloud storage, and mobile app access, the research now delivers the deployed architecture. The system boasts a fingerprint-secured doorbell and outdoor camera for visitor verification, paired with a central Raspberry Pi hub. For uninterrupted functionality, power backup functionality avoids system failure during power outages, adding reliability. Security information is sent to a Firebase cloud database, featuring live logs, visitor photos, and camera streams accessible through an easy-to-use mobile app. This paper outlines the goals, technical complexities, and real-world applications of the prototype, in terms of home security, guest verification, and possible law enforcement application. It adds to the expanding body of IoT-based security systems by providing a mature and tested solution for secure and efficient access control in our networked world.

The architecture of the system involves several layers of security via fingerprint verification and camera image capture at points of entry to further identify and verify visitors. The Raspberry Pi acts as the central processing unit, controlling elements like the camera, fingerprint reader, and cloud storage. Secure data is logged through Dropbox, providing tamper-proof records that can be accessed through a mobile app. Real-time alerts facilitate remote monitoring and management, enhancing the reliability and use of the system [3].

2.MOTIVATION

More than ever, as digital transformation changes every aspect of daily life, the concern for secure and reliable access control is foremost in the minds of homeowners and organizations alike. The demand for contactless yet intelligent security systems has prompted the creation of smart solutions that go beyond the usual locks and keys. Thus, this project seeks to develop a modern access

system for doors that integrates with the cloud to improve security and usability alike through mobile-based remote control and real-time monitoring.

The system provides strict access control through cloud services coupled with biometric authentication and camera surveillance while minimizing physical interaction. The solution remains viable and economical to set up by making use of reasonably priced platforms like Raspberry Pi and tools such as Android Studio and Firebase. This research is fueled by the aspirations to provide safety, facilitate access management, and enable future innovations in Cloud-based smart security systems.

3.LITERATURE REVIEW

Table 1: Literature

Authors	Applicat-ions	Pros	Cons
Arka A,et al.,2023	IOT Smart Home (Household Task)	The system is designed to be user-friendly, allowing even non-technical users to set up and manage it easily.	While easy to install for smaller setups, expanding the system to larger areas or integrating many devices may require additional components and technical expertise.
Amin I, et al.,2024	Remote management (Household Appliances)	Scalability: The model allows easy expansion by supporting additional devices and networks, making it flexible for future development.	Expanding the system introduces more potential points of attack. As more devices connect, the attack surface grows, making security management more challenging, despite built-in encryption.
Muhammad Z, et al.,2024	Secure Locker Systems	Secure OTP (One-Time Password) Generation	Generating and sending OTPs relies on both internet and mobile network availability. If the user's phone or email is inaccessible, they could be locked out of the system.

4.PROBLEM STATEMENT

We identified a problem that conventional locks, while widely used, have significant limitations in providing real-time visitor monitoring and effective remote management capabilities. These traditional systems lack the advanced features needed to offer users a secure, efficient, and convenient way to manage entry points. Without the integration of modern technology, users cannot remotely control or monitor access, nor can they receive real-time notifications or alerts regarding visitor activities. This gap in functionality highlights the need for an innovative solution that incorporates cloud-based technology, enhancing security, accessibility, and management of door access systems.

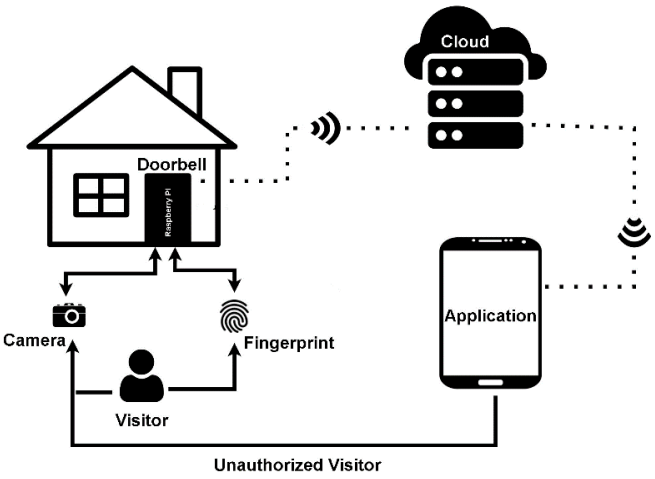
OBJECTIVE

1. To Develop a Doorbell System: Create a system that minimizes the need for physical interaction while enhancing security and convenience.
2. Ensure Real-Time Monitoring via a mobile application for enabling immediate identification of visitors.
3. To Implement Secure Biometric Algorithms for identity verification and authentication individuals can access the premises.

5.PROPOSED SYSTEM ARCHITECTURE

A visitor management system is an architecture through the key components involved in integrating an Arduino microcontroller, ultrasonic sensor, a Node MCU camera, and an Android-based mobile application. A visitor management system is therefore formed by using the Arduino as the central controller where it gathers input from the ultrasonic sensor. If a visitor is identified, the doorbell is activated and captures the picture of the visitor through the Node MCU camera, which then sends the image wirelessly through Wi-Fi to a mobile application. Through this Android-based app, house owners can get the picture of the visitor, get alerts, and view the visitor history. The system stores information in the cloud and retrieves images or logs safely.

6.SYSTEM ARCHITECTURE



The system architecture shown in the image illustrates a smart doorbell system integrated with advanced technologies like fingerprint scanning, video monitoring, and cloud-based data management. The system uses a Raspberry Pi as the main processing unit and integrates various components to provide secure, remote access control for a home. Here's a detailed breakdown of each part and how they interact.

6.1 Components

1. Raspberry Pi: The Raspberry Pi is the central hub of the entire system. It acts as the controller, managing interactions between hardware components like the camera, fingerprint scanner, and the cloud (Firebase). The Raspberry Pi is connected to the internet via Wi-Fi, allowing it to communicate with the cloud for data synchronization and management. .It processes fingerprint data, sends it to Firebase for authentication, and manages access control by either granting or denying entry based on the response from the cloud database.

2. Door-Bell with Fingerprint
   a. The doorbell is equipped with a fingerprint scanner, which acts as a primary security measure.

   b. When someone presses the doorbell, they are prompted to provide their fingerprint for verification.

   c. The fingerprint data is sent to the Raspberry Pi, which processes it and cross-checks it with the authorized database in Firebase.

   d. If the fingerprint matches, the system allows access; otherwise, it records the attempt as unauthorized.

3. Camera
   The camera captures images or live video feeds of individuals using the doorbell. It provides visual evidence of people approaching the door, which is useful for security purposes. If an unauthorized access attempt is detected (e.g., a fingerprint that doesn't match), the camera captures an image of the person and uploads it to Firebase for storage in the "Unauthorized Database." This feature enhances security by keeping a record of potential intruders and notifying the homeowner through the connected mobile application.

4. Screen (Optional Component)
   The system may include a small screen connected to the Raspberry Pi to display information, such as: Confirmation messages like "Access Granted" for authorized users. Warnings like "Access Denied" or "Unknown Fingerprint" for unauthorized attempts. A live feed from the camera showing who is at the door.

5. Wi-Fi Connectivity
   a. The Raspberry Pi connects to the home Wi-Fi network to communicate with Firebase and the mobile application.

   b. Wi-Fi connectivity allows the system to send and receive data in real-time, such as uploading images and logs to Firebase and sending notifications to the user's mobile device.

   c. It also ensures that the user can monitor and control the system remotely through the mobile application.

6. Firebase Cloud (Cloud Integration)
   Firebase is a cloud-based platform that provides the following features for this system: Data Storage: Firebase stores user data, access logs, and images of individuals accessing the system.

   a. Authorized Users and Logs Database: This database stores information about authorized users (fingerprint data) and logs all successful access attempts for record-keeping.

   b. Unauthorized Database: This separate database stores information and images of failed access attempts, capturing details of individuals whose fingerprints did not match any record.

   c. Authentication: Firebase can verify fingerprints by matching them with stored data to determine if an individual is authorized.

   d. Real-Time Synchronization: Firebase allows real-time data updates, so when someone uses the doorbell, the information is instantly processed,

logged, and sent to the user's mobile application.

7. Mobile Application
The mobile application serves as the user interface for managing and monitoring the system remotely

   a. Real-Time Notifications: The application sends instant notifications to the user when someone presses the doorbell. It notifies users of both authorized and unauthorized attempts, providing security alerts if necessary.

   b. Live Video Feed: The app allows the user to view a live video feed from the camera, enabling them to see who is at the door from anywhere.

   c. User Management: The app provides functionality for the user to add, modify, or remove fingerprints and manage authorized users directly through the application.

   d. Log Access: Users can view logs of all access attempts (both authorized and unauthorized) stored in Firebase, providing a history of events.

6.2 Workflow Summary

a) Doorbell Activation: When someone presses the doorbell, the fingerprint scanner activates and captures the person's fingerprint.
b) Verification: The Raspberry Pi processes the fingerprint data and checks it against the authorized database stored in Firebase. If a match is found, access is granted, and the event is logged in the "Authorized Users and Logs" database. If no match is found, the system records the attempt as unauthorized, captures an image using the camera, and stores it in the "Unauthorized Database".
c) Real-Time Updates: The Raspberry Pi sends information about the access attempt to the mobile application, which notifies the user immediately. The user can then choose to monitor the live video feed, access logs, or manage user information through the app.
d) Remote Management: Users can control and monitor the system remotely using the mobile application, allowing them to maintain security even when they are not at home.

7.METHODOLOGY

To develop a secure access control system based on biometric authentication, specifically using fingerprint recognition and a decision tree algorithm for making intelligent access decisions. The system will capture the fingerprint of a visitor, process it for matching against pre-stored templates, and then apply a decision tree to determine whether access should be granted based on the analysis of biometric data and other relevant visitor features.

ALGORITHM

Finger Template Matching Algorithm:

Step 1: System Initialization

The smart doorbell system is initialized, including the fingerprint scanner, Raspberry Pi, and mobile application.

The system establishes a connection to the cloud database (Firebase) for real-time synchronization.

Step 2: Capture Fingerprint

When a visitor presses the doorbell, they are prompted to place their finger on the fingerprint sensor.

The system captures the image of the fingerprint using the sensor.

Step 3: Pre-process Fingerprint

The captured fingerprint is processed to enhance image quality, reducing noise and improving contrast.

Key fingerprint features (such as ridges and minutiae points) are extracted to create a fingerprint template.

Step 4: Compare with Stored Templates

The processed fingerprint template is compared against pre-stored templates in the cloud database (Firebase).

The comparison uses pattern-based or minutiae-based algorithms to check for similarities.

Step 5: Matching Decision

If the similarity score exceeds a predefined threshold, the fingerprint is considered a match.

If no match is found or the score is below the threshold, access is denied.

Step 6: Access Decision

If a match is found, the system grants access, unlocks the door, and logs the successful attempt in Firebase.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03372
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

If no match is found, the system records the event as unauthorized and sends a notification to the user via the mobile application.

Step 7: End Process

The system returns to its idle state, ready for the next access attempt.

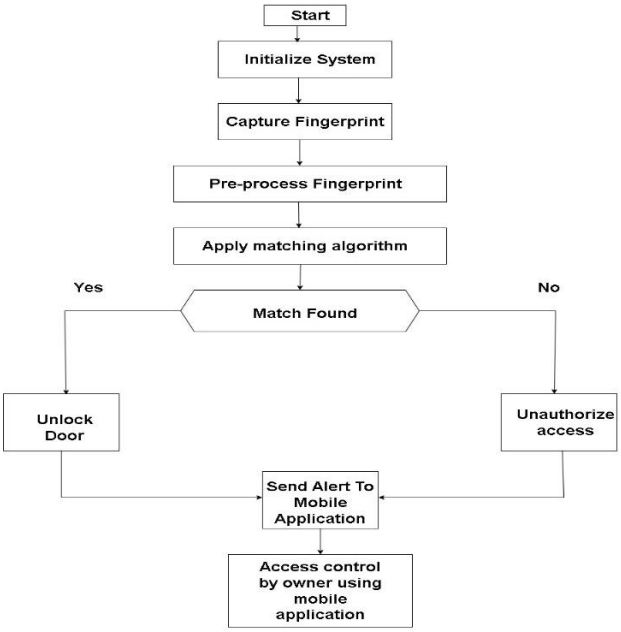


Figure 2. Flowchart

8.FUTURE SCOPE

Motion Detection: Incorporating motion detection capabilities to provide real-time alerts and enhance security when movement is detected near the entry point.

Face Recognition: Implementing facial recognition technology for accurate and efficient visitor identification, improving security measures.

9.RESULTS AND OUTCOMES

In a controlled environment trial, secure your entryway using a cloud-based door access system was implemented with success. The combination of fingerprint authentication, camera surveillance, and cloud-based data logging culminated in an effective and secure smart door access mechanism.

Key Results: The R301 fingerprint sensor authenticated registered users with high accuracy. The average response time for fingerprint matching was less than 2 seconds.

Camera Integration: The system stored pictures of visitors on Firebase cloud storage, thus generating visual logs with timestamps.

Mobile App Control: The Android application allowed users to ascertain the door activity and manipulate the latch (ON/OFF) without any contact.

Cloud Logging: All access events such as valid/invalid attempts were logged remotely on the cloud in real-time with the corresponding images.

System Reliability: The system showed flawless performance during various test scenarios exhibiting good behavior with all expected and edge-cases inputs.

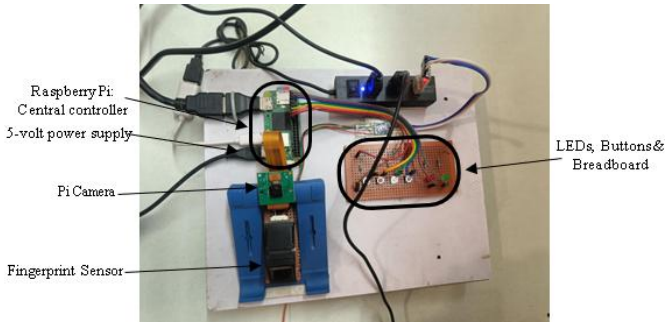
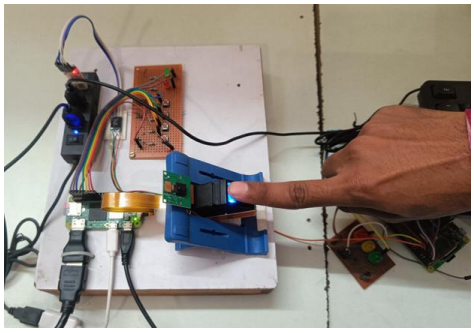


Figure 3: Hardware Setup with Fingerprint Sensor and Pi Camera

- Raspberry Pi: Central controller, located at the top center, connected via GPIO pins to peripherals, powered by a 5V adapter.
- Fingerprint Sensor: R301 model, mounted on a blue stand at the bottom center, connected to Raspberry Pi for biometric authentication.
- Pi Camera: 5-megapixel module, fixed on the blue stand above the fingerprint sensor, linked via CSI ribbon cable to capture images.
- 5V Power Supply: Positioned at the top right, connected to a power strip with a blue LED, supplying power to the Raspberry Pi.
- LEDs and Buttons: On a breadboard to the right, includes three buttons (add, delete, verify fingerprint) and a green LED for successful matches.
- Wiring: Multicolored jumper wires connect the Raspberry Pi to the breadboard, fingerprint sensor, and camera, ensuring organized data transfer.
- Additional Peripherals: HDMI cable and USB cables connected to the Raspberry Pi, likely for display output and setup purposes.

1. Enrolling new fingerprint:



International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03372
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

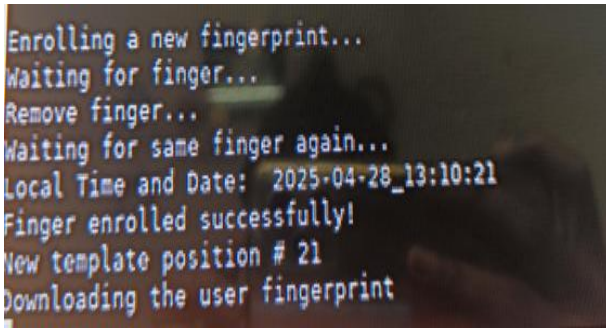
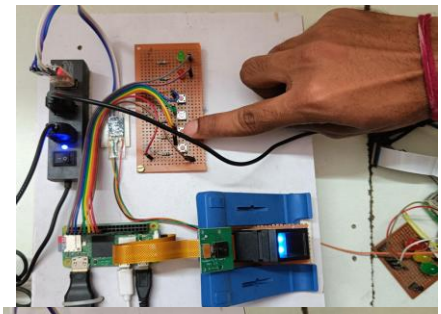


Figure 4: Fingerprint Enrolling

When the user presses Button 1, the fingerprint sensor (R301) is activated, and the user is prompted to place their finger. The Raspberry Pi processes the scanned data, generates a digital fingerprint template, and stores it locally.

2. Delete the fingerprint:



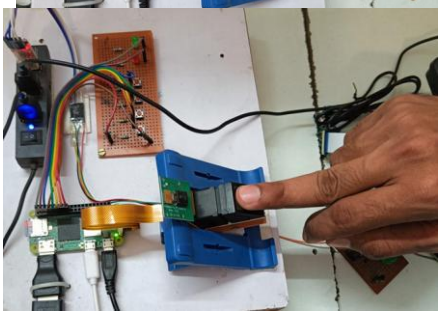
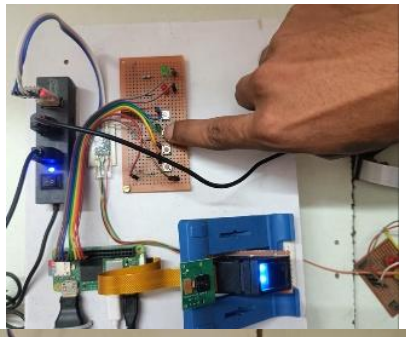


Figure 5: Fingerprint Deletion

When Button 2 is pressed, the system enters delete mode and prompts the user to place their finger on the sensor. If the fingerprint matches an existing template, the Raspberry Pi deletes it from memory.

3. Verification:



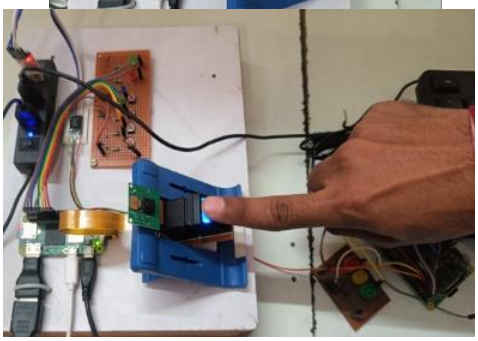


Figure 6: Fingerprint Deletion

When Button 3 is pressed, the system enters verification mode. The user places their finger on the sensor. If the fingerprint matches a stored template, the system grants access by unlocking the door. If there is no match, the system immediately clicks a photo using the camera and uploads the image to the cloud for monitoring or alert purposes.

4. Android application:

Figure 6: Android Application

The Android application is developed to monitor and manage the door access system remotely. When a user attempts to unlock the door using a fingerprint, the system verifies it in real time. If the fingerprint matches, access is granted; if not, the system automatically captures a photo of the person and uploads it to **Dropbox Cloud**. The app retrieves this image and displays it along with the timestamp. It also sends an instant notification to the user about the unauthorized access attempt. The application provides a simple and user-friendly interface where users can view logs, check alerts, and monitor entries from anywhere, ensuring enhanced security and real-time response.

Features of Camera Hardware:

A 5-Megapixel Camera Module has been integrated into the Raspberry Pi through CSI (Camera Serial Interface) as part of a smart surveillance function in the suggested system. The camera was capable of taking images of persons entering home real-time monitoring and logging in the cloud.

Key Specifications:

Feature	Specification
Sensor	5-Megapixel CMOS Sensor
Photo Resolution	Up to 2592 x 1944 pixels
Interface	CSI (Camera Serial Interface) — direct Pi connection
Lens	Fixed Focus Lens
Form Factor	Compact: 25mm x 20mm x 9mm

Application in System: For capturing image on fingerprint scan or on press of doorbell images uploaded to Firebase Cloud for secure logging and remote access Application integrated to display current visitor images via mobile app.

10.CONCLUSION

The Smart Doorbell System effectively combines biometric, face capture, cloud data storage, a mobile application, and a power backup feature to provide a reliable and secure entry solution. By leveraging cloud storage, the system ensures that visitor data is securely stored and accessible, offering post-conflict proof and accurate identification. The inclusion of a battery backup guarantees continuous operation even during power outages, enhancing the system's reliability. The mobile application offers users convenient control and access, enhancing overall user experience and accessibility. The system’s applications extend beyond residential use to commercial and industrial settings, showcasing its versatility and scalability. This comprehensive solution not only provides robust security but also meets modern demands for convenience and safety in various environments.

11.REFERENCES

[1]. Arka A, Saroj H, Rayith B, Shuvadeep P, Sourav H, Jayanta P, Arindam D, "Design and Implementation of an IoT-ased Smart Home Automation System in Real-World Scenario"In EAI Endorsed Transactions on Internet of Things, Volume 10, pages 1-8, 2024, doi:10.4108/etiot.6201.

[2]. Amin S. Ibrahim, Waelm. F, Abdel-Rehim ,Ahmedm.Abbas ,Ashraf Mohamedali Hassan, Ahmed Emam and Saeed Mohsen, "Design and Implementation of a Pilot Model for IoT Smart Home Networks," IEEE Access, vol. 11, pp. 59701–59718, June 2023, doi:10.1109/ACCESS.2023.3282095.

[3]. Muhammad Imran Zulfiqar , Ijaz Younis," Enhanced security paradigms: Converging IoT and

biometrics for advanced locker protection," in IEEE Internet of Things Journal, IEEE, 2024, pp. 1–10, doi :10.1109/JIOT.2024.3432282.

[4]. H. -B. Kim, N. Choi, H. -J. Kwon and H. Kim, "Surveillance System for Real-Time HighPrecision Recognition of Criminal Faces From Wild Videos," in IEEE Access, vol. 11, pp. 56066-56082, 2023, doi:10.1109/ACCESS.2023.3282451.

[5]. L. P. O. Paula, N. Faruqui, I. Mahmud, M. Whaiduzzaman, E. C. Hawkinson and S. Trivedi, "

A Novel Front Door Security (FDS) Algorithm Using GoogleNet-BiLSTM Hybridization," in IEEE Access, vol. 11, pp. 19122-19134, 2023, doi:10.1109/ACCESS.2023.3248509.

[6]. Z. Huang, J. Zhang and H. Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis:

A Multi-Task Learning Framework and a New Benchmark," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 6, pp. 7917-7932, 1 June 2023, doi: 10.1109/TPAMI.2022.3217882.

[7]. A. Krishnan and T. Thomas, "Finger Vein Recognition Based on Anatomical Features of Vein Patterns,

" in IEEE Access, vol. 11, pp. 39373-39384,23, doi:10.1109/ACCESS.2023.3253203.

[8]. Y. Huang, H. Ma and M. Wang, "Multimodal Finger Recognition Based on Asymmetric Networks With Fused Similarity," in IEEE Access, vol. 11, pp. 17497-17509, 2023, doi: 10.1109/ACCESS.2023.3242984. International Journal of Research Publication and Reviews, Vol 5, no 3, pp 2033-2038 March 2024 2038.

[9]. C. -Y. Lin, F. -J. Chen, H. -F. Ng and W. -Y. Lin, "Invisible Adversarial Attacks on Deep Learning- Based Face Recognition Models," in IEEE Access, vol. 11, pp. 51567-51577, 2023, doi:10.1109/ACCESS.2023.3279488

[10]. D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G Internet of Things: A comprehensive survey," IEEE Internet Things J., vol. 9, no. 1, pp. 359–383, Jan. 2022.