AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 4(2025)
www.ajmimc.com

IOT BASED SECURE BIOMETRIC AUTHENTICATION SYSTEM

[1] Dr. V.Sandeep Kumar, [2] R. Sneha, [3] M. Bhanu Prasad, [4] N. Ranjith Kumar Reddy,

[1] *Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

[2,3,4,5] *B. Tech Student, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

ABSTRACT

In today's interconnected world, security and identity verification are critical for safeguarding personal, corporate, and governmental data. Traditional password-based authentication systems are increasingly vulnerable to attacks such as hacking, phishing, and password theft. To overcome these limitations, this project proposes an IoT-Based Secure Biometric Authentication System that uses fingerprint or facial recognition integrated with IoT technology for real-time verification and monitoring. The system uses a biometric sensor to capture and verify the user's identity, and communicates with a cloud-based IoT platform to store and validate authentication data securely. This ensures that only authorized users can access restricted areas or systems. The proposed design enhances security, scalability, and accessibility while eliminating the weaknesses of traditional authentication methods.

Keywords: Biometric Authentication, Fingerprint Recognition, Cloud Security, NodeMCU, Real-Time Verification.

I. INTRODUCTION

Security systems are an integral part of modern digital and physical infrastructures. Conventional authentication techniques such as PINs or passwords suffer from vulnerabilities including weak password selection and unauthorized access. Biometric authentication, which relies on unique physiological traits like fingerprints, iris, or facial patterns, offers a more secure and reliable solution. This project integrates biometric technology with IoT, allowing real-time authentication, data storage, and monitoring through cloud servers. The IoT network ensures that biometric data and access logs are accessible remotely for authorized administrators. Applications include smart homes, offices, ATMs, vehicle systems, and industrial security setups. The system not only enhances access control but also introduces data-driven decision-making for better security management.

II. LITERATURE SURVEY

1. Singh et al. (2019) – Fingerprint-Based IoT Authentication System

Singh et al. implemented a fingerprint authentication system using Arduino and cloud integration. Their model achieved basic user verification through Wi-Fi but lacked encryption mechanisms to ensure data privacy during transmission.

2. Kumar and Rao (2020) – Secure IoT Access with Biometric Verification

Kumar and Rao proposed an IoT-based access control mechanism using a fingerprint sensor and Firebase database. Although real-time monitoring was successful, the system faced delays in large-scale implementations due to limited network bandwidth.

3. Ahmed et al. (2021) – Facial Recognition Security over IoT Networks

Ahmed et al. developed a Raspberry Pi-based face recognition system that integrated OpenCV with IoT platforms. The design demonstrated high accuracy but required constant high-speed internet connectivity for cloud verification.

4. Das and Banerjee (2022) – Biometric Encryption and Cloud Security

Das and Banerjee presented a model that combined biometric data with cryptographic techniques before transmitting it to IoT servers.

This hybrid approach improved data protection but increased system complexity and cost.

5. Patel and Mehta (2023) – Smart Home Authentication using IoT Biometrics

Patel and Mehta built an IoT-based smart lock that used a fingerprint scanner connected to NodeMCU and Blynk cloud. Their system efficiently controlled access for multiple users and provided remote monitoring through a mobile app, ensuring convenience and security.

III. EXISTING SYSTEM

The existing security systems rely mainly on RFID cards**,** passwords, or PIN codes. These methods are susceptible to theft, duplication, or human error. Even though some systems use standalone biometric authentication, they often lack network connectivity or cloud integration for centralized management. Furthermore, the absence of data encryption makes them vulnerable to hacking or spoofing attacks. Therefore, there is a need for a secure IoT-integrated biometric system that ensures authentication integrity and allows remote monitoring.

IV. PROPOSED SYSTEM

The proposed IoT-Based Secure Biometric Authentication System integrates biometric sensors (fingerprint/facial recognition) with IoT cloud platforms to achieve secure and remote identity verification. The system uses:

- **Biometric Sensor (R307 or R503)** for fingerprint detection.
- **Microcontroller (NodeMCU/ESP32)** for control and IoT communication.
- **Cloud Server (ThingSpeak, Firebase, or AWS IoT)** for secure data storage.
- **Encryption Algorithm (AES/SHA-256)** to secure biometric data transmission.
- **Relay or Lock Mechanism** to control physical access based on authentication results.

When a user attempts access, the biometric sensor captures and verifies the fingerprint locally. If validated, the data is encrypted and transmitted via Wi-Fi to the cloud, where access logs are updated in real-time. If an unauthorized attempt is detected, an alert message or email is sent to the administrator. This ensures multi-level security and remote supervision.

V. SYSTEM ARCHITECTURE

- **Biometric Sensor** – Captures and verifies the user's fingerprint or face.
- **Microcontroller (NodeMCU/ESP32)** – Processes sensor input and connects to the internet.
- **Wi-Fi Module (Integrated)** – Transmits authentication data securely to the IoT cloud.
- **Cloud Database (Firebase/ThingSpeak)** – Stores authentication logs and user details.
- **Relay-Controlled Door Lock** – Grants or denies access.
- **Web/Mobile Interface** – Displays access history and alerts.

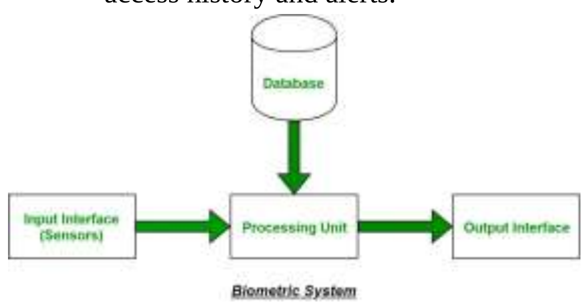

Fig.5.1: System architecture

ARUDINO:

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmega microcontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/output pins, all on a single chip. Unlike, say, a Raspberry Pi, it's designed to attach all kinds of sensors, LEDs, small motors and speakers, servos, etc. directly to these pins, which can read in or output digital or analog voltages between 0 and 5 volts. The Arduino connects to your computer via USB, where you program it in a simple language (C/C++, similar to Java) from inside the free Arduino IDE by uploading your compiled code to the board. Once programmed, the Arduino can run with the USB link back to your computer, or stand-alone without it — no keyboard or screen needed, just power.

Starting clockwise from the top center:

- Analog Reference pin (orange)
- Digital Ground (light green)
- Digital Pins 2-13 (green)
- Digital Pins 0-1/Serial In/Out - TX/RX (dark green) - These pins cannot be used for digital i/o (Digital Read and Digital Write) if you are also using serial communication (e.g. Serial.begin).
- Reset Button - S1 (dark blue)
- In-circuit Serial Programmer (blue-green)
- Analog In Pins 0-5 (light blue)
- Power and Ground Pins (power: orange, grounds: light orange)
- External Power Supply In (9-12VDC) - X1 (pink)
- Toggles External Power and USB Power (place jumper on two pins closest to desired supply) - SV1 (purple)
- USB (used for uploading sketches to the board and for serial communication between the board and the computer; can be used to power the board) (yellow)

DIGITAL PINS

- In addition to the specific functions listed below, the digital pins on an Arduino board can be used for general purpose input and output via the pin Mode(), Digital Read(), and Digital Write() commands. Each pin has an internal pull-up resistor which can be turned on and off using digital Write() (w/ a value of HIGH or LOW, respectively) when the pin is configured as an input. The maximum current per pin is 40mA.

ANALOG PINS

In addition to the specific functions listed below, the analog input pins support 10-bit analog-to-digital conversion (ADC) using the analog Read() function. Most of the analog inputs can also be used as digital pins: analog input 0 as digital pin 14 through analog input 5 as digital pin 19. Analog inputs 6 and 7 (present on the Mini and BT) cannot be used as digital pins.

VI. IMPLEMENTATION

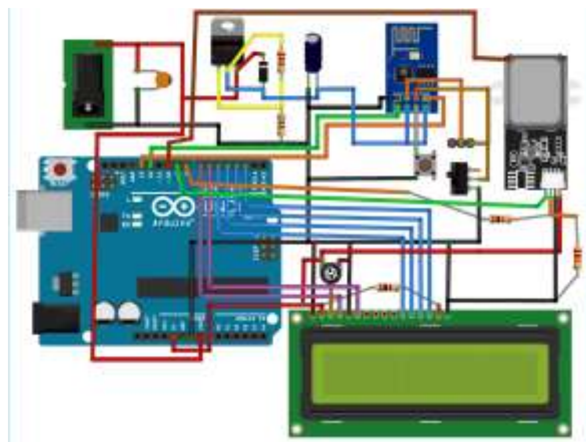

FIG. 6.1: Circuit diagram for proposed model

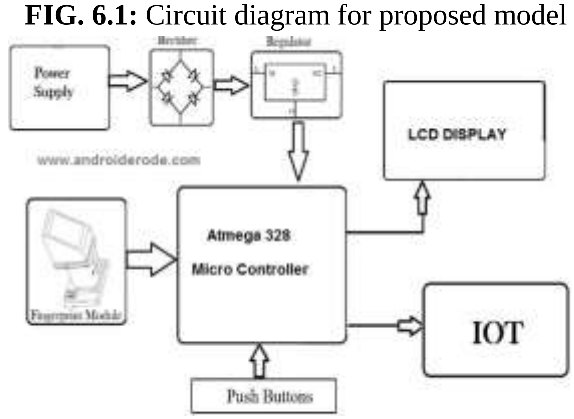

FIG. 6.2: Block diagram

The IoT-Based Secure Biometric Authentication System is a modern identity verification solution that combines biometric technology with Internet of Things (IoT) connectivity to ensure high-level security and remote accessibility. The system uses a biometric sensor, such as a fingerprint**,** facial recognition, or iris scanner, connected to a microcontroller or microprocessor (e.g., Arduino, NodeMCU, or Raspberry Pi) to capture and verify the user's unique biological traits. Once a biometric scan is performed, the system compares it with pre-stored data to authenticate the user. Upon successful verification, the system grants access or triggers specific actions, such as unlocking a door, logging into a system, or activating machinery. The authentication data and access logs are securely transmitted to a cloud platform using IoT protocols like MQTT or HTTP, enabling remote monitoring and management by authorized personnel. Advanced encryption techniques are implemented to protect biometric data during transmission and storage, ensuring privacy and security. In case of unauthorized access attempts, the system can send instant alerts via email, SMS, or a mobile application**.** This IoT-based biometric authentication system provides a robust, scalable, and tamper-resistant solution for applications in smart homes, offices, banking, and industrial security systems, combining convenience with enhanced protection against identity theft and unauthorized access.

VII. CONCLUSION

The IoT-Based Secure Biometric Authentication System provides a highly secure, scalable, and real-time access control mechanism. By combining biometric authentication with IoT and cloud computing**,** the system ensures reliable verification and remote monitoring. It eliminates the risks of password misuse and card duplication. The design can be easily adapted for smart homes, office entry systems, ATMs, or vehicle locks, providing a universal and modern security solution.

VIII. FUTURE SCOPE

- Integration of multi-factor authentication (biometric + OTP) for enhanced security.
- Implementation of blockchain technology to improve data integrity.
- Edge computing for faster local authentication and reduced latency.
- Mobile app-based control for adding/removing authorized users.
- Facial and iris recognition for advanced multi-biometric verification.

IX. REFERENCES

[1].Dimitrios P. Glaroudis and Athanasios C. Iossifides and Periklis Chatzimisios, . "Survey, comparison and research challenges of IoT application protocols for smart farming".Comput. Networks 168 (2020).

[2].Soraya Sinche and Duarte M. G. Raposo and Ngombo Armando and André Rodrigues and Fernando Boavida and Vasco Pereira and Jorge Sá Silva, . "A Survey of IoT Management Protocols and Frameworks".IEEE Commun. Surv. Tutorials 22, no.2 (2020): 1168–1190.

[3].Arun Ross, , Sudipta Banerjee, and Anurag Chowdhury. "Security in smart cities: A brief review of digital forensic schemes for biometric data".Pattern Recognition Letters 138 (2020): 346 - 354.

[4].Sathyan Munirathinam, "Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT)," Adv. Comput. 117 (2020): 129–164, doi:10.1016/bs.adcom.2019.10.010, [5].Gulraiz J. Joyia et al., "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain," J. Commun. 12, no. 4 (2017): 240– 247, doi:10. 12720/jcm.12.4.240-247,

[6].Muhammad Junaid Farooq and Quanyan Zhu, "On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT)," IEEE Trans. Wireless Communications 17, no. 4 (2018): 2618–2632,

Received: 28-09-2025 | Accepted: 03-11-2025 | Published: 10-11-2025 |

[7].Rubin Zheng, Haowei Wang, and Jingzhu Zhao, "A Unified Management Framework for EIoT Systems Based on Metadata and Event Detection," IEEE Access 7 (2019): 112629–112638,