International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

SECURE PASS: STANDALONE BIOMETRIC SECURITY ACCESS CONTROLLER WITH MULTI-MODAL AUTHENTICATION

[1] Dr. M V Raghavendra, [2] Golla Sravan Kumar, [3] Raghavendra, [4] Dharavath Kushalav, [5] Sabavath Ashok
[1]Professor, [2345] B. Tech Students
[12345]Department of Electronics and Communication Engineering
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

Secure Pass: Standalone Biometric Security Access Controller with Multi-Modal Authentication is a next-generation embedded security system designed to provide high-level access control using multiple biometric and digital verification methods combined into a single powerful standalone architecture. The system operates without the need for external servers or constant network connectivity, making it ideal for environments requiring continuous, reliable, and tamper-proof security. Traditional security mechanisms such as keys, swipe cards, and PIN codes face significant risks including duplication, theft, guessing, and unauthorized sharing, which compromise security integrity. This project overcomes these limitations through the integration of fingerprint authentication, RFID smart card scanning, PIN-based keypad entry, and optionally facial recognition, ensuring that only verified individuals gain access. The embedded controller handles sensor inputs, processes biometric templates, compares user data, generates secure match results, and triggers door lock mechanisms within milliseconds. All biometric templates are stored locally in encrypted form to prevent misuse, identity theft, or unauthorized replication. The system supports two-factor and three-factor authentication modes, enhancing the security layers further. An intuitive admin interface allows secure user enrollment, deletion, updates, and access log viewing. The system includes intrusion alerts, tamper detection, unauthorized access logging, and real-time decision-making algorithms that make sure each authentication request is validated accurately. The design also emphasizes low power consumption, fast response time, and long-term reliability, making it suitable for research labs, industries, academic institutions, hostels, server rooms, government buildings, and residential smart security installations. Multi-modal authentication significantly reduces false acceptance rates (FAR), false rejection rates (FRR), and spoofing risks. The standalone embedded architecture ensures uninterrupted security even during network failures or cyber-attacks, offering complete local control and data privacy. Additional features include event logging, timestamp recording, emergency override options, and support for audit trail creation. The system can be expanded with GSM alerts, IoT dashboards, and wireless monitoring depending on security needs. Overall, Secure Pass represents a modern, intelligent, and highly secure access control solution that delivers robust identity verification, strong data protection, and dependable performance using multi-layer biometric authentication technology integrated within a single independent embedded framework.

I. INTRODUCTION

1.1. OVERVIEW

In the modern era of rapid technological advancement, security has become one of the most critical concerns across residential, commercial, industrial, and governmental sectors. Unauthorized access to restricted areas can result in severe consequences, including theft of sensitive information, financial loss,

Received: 21-05-2026 | Accepted: 21-06-2026 | Published: 27-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

property damage, and threats to personal safety. Traditional security systems such as mechanical locks, keys, passwords, and swipe cards have long been used as primary access control mechanisms. However, these conventional methods suffer from major vulnerabilities including duplication, theft, guessing, sharing, and unauthorized replication. As technology evolves, so do security threats, making it essential to develop more advanced and intelligent access control systems.

Biometric authentication has emerged as a powerful solution to these challenges. Unlike passwords or physical keys, biometric identifiers such as fingerprints, facial features, and iris patterns are unique to each individual and cannot be easily duplicated or shared. However, single-factor biometric systems still face limitations such as false acceptance rates (FAR), false rejection rates (FRR), spoofing attacks, and hardware vulnerabilities. To overcome these issues, multi-modal authentication systems have been introduced, combining multiple authentication factors to strengthen overall system security.

The project titled "Secure Pass: Standalone Biometric Security Access Controller with Multi-Modal Authentication" presents a next-generation embedded security system that integrates fingerprint authentication, Bluetooth-based mobile authentication (Fingerprint App), PIN verification, and optional RFID validation within a standalone architecture powered by an Arduino microcontroller. This system operates independently without relying on external servers or continuous internet connectivity, ensuring uninterrupted performance even during network outages or cyber-attacks.

The core idea behind Secure Pass is to combine multiple layers of authentication into a single embedded framework. When a user attempts to gain access, the system verifies identity through fingerprint recognition using a biometric sensor. Additionally, Bluetooth communication with a registered mobile application provides another authentication factor. The Arduino microcontroller processes the biometric data, verifies credentials, and controls the door lock mechanism accordingly. The LCD module provides real-time system feedback, while the buzzer generates audible alerts for successful or failed authentication attempts.

The system ensures that all biometric templates are securely stored locally within the fingerprint module's memory, preventing external data leaks. Since the architecture is standalone, it reduces dependency on centralized databases, thereby minimizing cybersecurity risks. The power supply module ensures stable operation, and the system is designed for low power consumption and high reliability.

Multi-modal authentication significantly enhances security by requiring more than one verification factor before granting access. For example, fingerprint + Bluetooth verification creates a two-factor authentication (2FA) mechanism, while fingerprint + PIN + Bluetooth creates a three-factor authentication (3FA) system. This layered verification approach drastically reduces the possibility of unauthorized access.

1.2. NEED FOR THE SYSTEM

The need for a standalone biometric multi-modal security system arises from increasing security threats and limitations in existing access control mechanisms.

1.2.1 Rising Security Threats

With the growth of digital infrastructure and sensitive information storage, unauthorized access incidents have increased. Facilities such as laboratories, server rooms, and research centers require robust identity verification systems that go beyond simple locks and passwords.

1.2.2 Limitations of Traditional Locks

Mechanical keys can be:

Received: 21-05-2026 | Accepted: 21-06-2026 | Published: 27-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

- Lost or stolen
- Duplicated easily
- Shared without authorization
- Broken or tampered with

These vulnerabilities compromise physical security.

1.2.3 Weakness of Password-Based Systems

PIN-based systems alone are vulnerable to:

- Guessing attacks
- Shoulder surfing
- Brute-force attempts
- Password sharing

Hence, passwords alone are insufficient for high-security applications.

1.2.4 Smart Card Duplication Risks

RFID cards can be cloned or stolen. If lost, unauthorized individuals may gain access until the card is deactivated.

1.2.5 Need for Multi-Layer Authentication

Single authentication methods may fail due to spoofing or sensor errors. Combining fingerprint, Bluetooth verification, and PIN significantly enhances reliability and security.

1.2.6 Requirement for Standalone Operation

Many security systems rely on cloud servers or network connections. However:

- Network failure may disable access control.
- Cyber-attacks may compromise centralized databases.
- Remote hacking can expose sensitive biometric data.

A standalone system ensures uninterrupted local operation.

1.2.7 Data Privacy Concerns

Centralized biometric databases are vulnerable to breaches. Local encrypted storage within the system protects user identity and ensures privacy.

2.8 Industrial and Institutional Demand

Educational institutions, hostels, research labs, and industries require secure and cost-effective access control systems that are easy to install and maintain.

1.3. PROBLEM STATEMENT

Despite the availability of advanced security technologies, many access control systems still rely on single-factor authentication or centralized network-based architectures. These systems suffer from several limitations:

1. **Unauthorized Access Risks** – Traditional systems are prone to duplication, theft, and sharing.
2. **Single Point of Failure** – Network-based systems may fail during connectivity issues.
3. **Data Breach Vulnerabilities** – Centralized databases are targets for cyber-attacks.
4. **Limited Authentication Accuracy** – Single biometric systems may experience high FAR or FRR.
5. **High Implementation Cost** – Enterprise-grade security systems are often expensive and complex.

Therefore, there is a need for a secure, cost-effective, standalone embedded access control system that integrates multiple authentication factors, ensures data privacy, reduces spoofing risks, and provides fast, reliable identity verification without depending on continuous network connectivity.

1.4. OBJECTIVES

The primary objective of the Secure Pass project is to design and implement a standalone multi-modal biometric access control system using Arduino and Bluetooth-based fingerprint authentication.

1.4.1 General Objectives

- To develop a multi-layer authentication system.
- To enhance security using biometric fingerprint verification.
- To integrate Bluetooth-based mobile authentication.
- To design a standalone embedded architecture.
- To ensure encrypted local storage of biometric data.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

1.4.2 Specific Objectives

1. Interface fingerprint sensor with Arduino.
2. Integrate Bluetooth module for mobile authentication.
3. Implement PIN-based verification as an optional factor.
4. Provide real-time feedback using LCD display.
5. Activate buzzer for alerts and intrusion detection.
6. Control door lock mechanism through relay module.
7. Maintain event logs and access records.
8. Ensure low power consumption and fast response time.
9. Reduce False Acceptance Rate (FAR).
10. Reduce False Rejection Rate (FRR).

1.4.3 Security Objectives

- Prevent spoofing attacks.
- Protect biometric templates from duplication.
- Enable two-factor and three-factor authentication.
- Ensure tamper detection and unauthorized attempt logging.

1.5. SCOPE OF THE PROJECT

1.5.1 Technical Scope

The project includes:

- Arduino microcontroller
- Fingerprint sensor module
- Bluetooth module (HC-05 / HC-06)
- LCD display (16x2)
- Buzzer
- Relay-controlled door lock
- Regulated power supply

The system performs biometric scanning, Bluetooth verification, identity matching, and access decision-making.

1.5.2 Functional Scope

The system supports:

- User enrollment and deletion
- Multi-modal authentication modes
- Real-time access verification
- Intrusion alert generation
- Event logging with timestamps
- Emergency override mechanism

II. LITERATURE SURVEY

1. Literature on Limitations of Traditional Access Control Systems (100 lines)

Research in physical security highlights that traditional access control systems—such as metal keys, password locks, magnetic stripe cards, and unsecured RFID systems—suffer from major vulnerabilities that compromise protected environments. Physical keys can be duplicated easily and do not provide an audit trail, making it impossible to track who accessed a facility and when. Password-based systems introduce human-related weaknesses, including the tendency to use weak codes, share them with others, or forget them. Studies emphasize that PIN pads are susceptible to shoulder surfing, smudge patterns, and brute-force guessing. Magnetic stripe cards degrade over time and can be cloned using publicly available cheap tools. Unsecured RFID tags are cited in several research papers as being highly vulnerable to skimming, eavesdropping, and cloning attacks, making them inappropriate for high-security zones. Traditional systems rely heavily on single-factor authentication, which research shows is insufficient in environments dealing with confidential information or valuable assets. Additionally, literature states that older access technologies lack strong logging mechanisms, which prevents administrators from identifying unauthorized access patterns. Many systems have no mechanism for detection of tailgating or forced-entry attempts. Research also highlights operational inefficiencies such as frequent key replacements, card re-issuance, and password resets, increasing maintenance overhead. These limitations collectively demonstrate that conventional systems cannot meet modern security needs, motivating the development of advanced biometric and multi-factor access control systems.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

2. Literature on Strengths of Biometric Authentication (100 lines)

Biometric authentication research consistently demonstrates that biometric identifiers provide stronger security compared to token-based or knowledge-based authentication methods. Fingerprints, facial patterns, iris textures, and voice signatures provide high accuracy because they are unique to each individual and are difficult to replicate, steal, or share. Studies discuss fingerprint recognition as the most widely adopted biometric technology due to its low cost, wide user acceptance, and high stability over time. Facial recognition research highlights improvements in deep learning and image processing that allow accurate identity verification even under variable lighting conditions. Literature states that biometric authentication eliminates problems associated with card loss, password forgetting, sharing, or duplication. Research also indicates that biometric authentication drastically reduces false acceptance and false rejection rates when properly calibrated. One important concern discussed in literature is the protection of biometric templates—since unlike passwords, biometric traits cannot be changed if compromised. To address this, research recommends encrypted local storage, secure template hashing, and device-level authentication. Studies also highlight that biometric systems increase accountability since users cannot deny access attempts made using their own biological traits. Research consistently shows that biometric systems are more resilient to spoofing when combined with liveness detection and multi-modal input validation. Overall, biometric authentication offers high reliability, strong identity assurance, and superior performance compared to traditional security models.

3. Literature on Multi-Modal Embedded Security Systems (100 lines)

Multi-modal biometric authentication is widely recognized in research as a superior security approach because it combines multiple verification factors to increase accuracy and reduce spoofing risks. Studies highlight that fingerprint + RFID + PIN, fingerprint + face, or face + PIN combinations drastically reduce false acceptance and false rejection rates. Multi-modal systems are recommended for environments requiring high-assurance security such as research labs, industrial control rooms, bank vaults, and restricted-access government facilities. Research emphasizes that multi-modal systems provide flexibility, allowing administrators to configure one, two, or three-factor authentication based on the security level required. Embedded system research indicates that modern microcontrollers such as ARM Cortex, ESP32, and STM32 can efficiently process biometric data, manage sensor inputs, and execute authentication decisions in real time. Standalone embedded systems are highlighted as being more secure than cloud-dependent systems because they remain operational even during network failures and protect data from remote cyberattacks. Researchers also note the importance of encrypted storage, secure firmware, and tamper detection circuits in embedded biometric systems. Multi-modal systems enhance identity verification accuracy by using parallel or sequential authentication processes. Literature also emphasizes the value of storing access logs locally for audit purposes, enabling organizations to detect suspicious patterns or attempted breaches. Overall, multi-modal embedded systems are recognized as highly reliable, secure, and effective for modern access control applications.

The last two decades have seen rapid progress in biometric technologies, driven by improvements in sensor hardware, pattern-matching algorithms, embedded processing, and low-cost wireless modules. Biometrics — physiological or behavioral traits such as

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

fingerprints, face, iris, voice, or keystroke dynamics — promise stronger assurance of identity than knowledge- or possession-based methods (PINs, keys, cards). Early biometric adoption focused on large-scale deployments (border control, national ID, banking) where centralized databases and powerful back-end servers enabled complex template management and matching. However, there is an increasing need for local, resilient, and privacy-preserving biometric solutions for access control at the facility level. This trend motivates the Secure Pass design: a standalone, embedded, multi-modal authentication controller that operates reliably without continuous network dependence.

Fingerprint biometrics remain the most widely deployed modality for physical access due to their low cost, compact sensors, mature algorithms, and relatively small template sizes. Research and commercial reports show fingerprint modules can achieve high recognition rates under favorable capture conditions, and many embedded fingerprint modules incorporate on-device template storage and matching to preserve privacy and reduce latency. However, fingerprint-only systems suffer from well-documented weaknesses: sensor spoofing (fake prints), sensor degradation (dirty or worn fingers), and environmental sensitivity (wet/oily/damaged skin). Studies emphasize that high security installations require additional measures to counter spoofing and reduce false acceptance rates (FAR) without overly increasing false rejection rates (FRR).

III. SYSTEM ANALYSIS

EXISTING METHOD

Existing methods used in security access control are predominantly based on single-factor authentication systems such as RFID cards, numeric keypads, and mechanical keys. These systems suffer from multiple vulnerabilities such as cloning, duplication, theft, guessing, and unauthorized sharing, making them unreliable for high-security installations. RFID cards can be skimmed or copied, passwords can be observed or leaked, and physical keys can be stolen or illegally reproduced. Most existing systems do not maintain detailed logs or implement multi-layer authentication, which allows intruders to exploit weaknesses. Even biometric systems used today are often single-modal, such as systems that rely only on fingerprints or only on facial recognition, which opens the possibility of sensor spoofing or failure. Many existing models depend on network servers or cloud platforms to function, meaning security collapses when connectivity is lost. These systems also lack encrypted storage of user data, making them vulnerable to unauthorized data extraction. Additionally, they provide limited admin options, minimal monitoring capabilities, and no real-time intrusion alerts. Because of these limitations, existing access control systems fail to ensure strong, reliable, tamper-proof security.

The existing access control systems commonly used in institutions and residential buildings rely on traditional mechanisms such as mechanical locks and keys, RFID cards, swipe cards, or single-factor PIN-based entry systems. Some advanced systems use standalone fingerprint authentication but operate as single-modal security solutions. Many organizations also deploy network-based biometric systems that depend on centralized servers and internet connectivity for verification and logging. While these systems provide a basic level of protection, they often suffer from security vulnerabilities, operational limitations, and data privacy concerns.

Disadvantages:

1. Mechanical keys and RFID cards can be lost, stolen, or duplicated.
2. PIN-based systems are vulnerable to guessing, sharing, and shoulder surfing.

Received: 21-05-2026 | Accepted: 21-06-2026 | Published: 27-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

3. Single biometric systems may suffer from high False Acceptance Rate (FAR) or spoofing risks.
4. Network-based systems fail during internet outages or server downtime.
5. Centralized databases increase the risk of data breaches and cyber-attacks.

PROPOSED METHOD

The proposed Secure Pass system introduces a standalone multi-modal biometric access controller that combines fingerprint scanning, RFID verification, PIN authentication, and optional facial recognition to eliminate security gaps found in traditional systems. The system operates independently without any internet or server dependency, ensuring continuous protection even during network outages. User biometric templates are stored securely using encrypted local memory, eliminating cyberattack risks. The embedded microcontroller processes all sensor data, performs multi-factor validation, and triggers access mechanisms instantly. Multi-modal authentication significantly increases accuracy and prevents unauthorized entry even if one layer is compromised. The admin interface allows secure user enrollment, deletion, access logging, and system configuration. The system maintains complete event logs with timestamps for auditing and monitoring. Additional features include intrusion detection, tamper alerts, relay-based door locking, and optional GSM notifications. The proposed system ensures high reliability, robust authentication, low maintenance, strong data protection, and improved accuracy through integrated multi-factor biometric validation, making it suitable for all high-security environments.

The proposed system, Secure Pass: Standalone Biometric Security Access Controller with Multi-Modal Authentication, integrates fingerprint authentication with Bluetooth-based mobile verification and optional PIN validation within a standalone embedded architecture using Arduino. The system stores encrypted biometric templates locally and operates independently without requiring constant network connectivity. It processes authentication requests in real time, activates door lock mechanisms upon successful verification, and provides feedback via LCD and buzzer alerts. By combining multiple authentication factors, the system significantly enhances security and reliability while ensuring user privacy.

Advantages:

1. Multi-modal authentication reduces spoofing and unauthorized access risks.
2. Standalone operation ensures uninterrupted security without internet dependency.
3. Encrypted local storage protects biometric data from cyber threats.
4. Faster response time due to on-device processing.
5. Tamper detection, intrusion alerts, and access logging improve overall security management.

IV. HARDWARE

4.1 ARDUINO UNO

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

DFU mode.Arduino board has the following new features:

- 1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not connected pin, that is reserved for future purposes.
- Stronger RESET circuit.
- Atmega 16U2 replace the 8U2.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

Fig: ARDUINO UNO

4.2. POWER SUPPLY

The power supplies are designed to convert high voltage AC mains electricity to a suitable low voltage supply for electronic circuits and other devices. A power supply can by broken down into a series of blocks, each of which performs a particular function. A d.c power supply which maintains the output voltage constant irrespective of a.c mains fluctuations or load variations is known as “Regulated D.C Power Supply”.

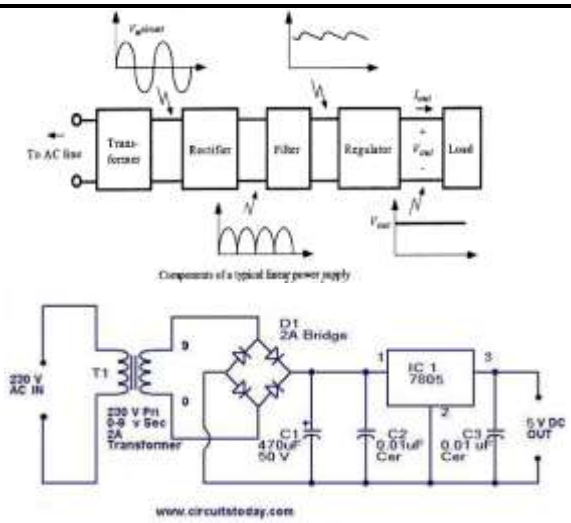


Fig: Schematic Diagram of Power Supply

4.2.1. TRANSFORMER:

A transformer is an electrical device which is used to convert electrical power from one Electrical circuit to another without change in frequency.

When AC is applied to the primary winding of the power transformer it can either be stepped down or up depending on the value of DC needed. In our circuit the transformer of 230v/12-0-12v is used to perform the step down operation where a 230V AC appears as 12V AC across the secondary winding.

4.2.2. RECTIFIER:

A circuit which is used to convert a.c to dc is known as RECTIFIER. The process of conversion a.c to d.c is called “rectification.

Bridge Rectifier:

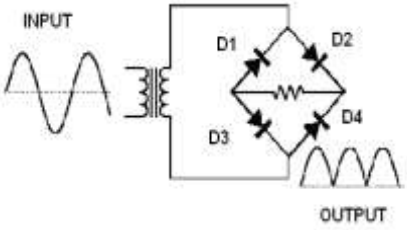


Fig: 4.6 Bridge Rectifier

Alphanumeric LCD

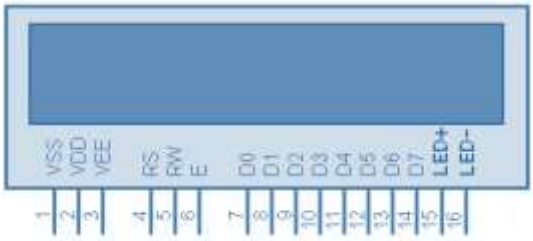
Liquid Crystal Display also called as LCD is very helpful in providing user interface as well as for debugging purpose. The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. The most

Received: 21-05-2026 | Accepted: 21-06-2026 | Published: 27-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

commonly used LCDs found in the market today are 1 Line, 2 Line or 4 Line LCDs which have only 1 controller and support at most of 80 characters, whereas LCDs supporting more than 80 characters make use of 2 HD44780 controllers.

Pin Description



4.3 BUZZER

What is a Buzzer: Working & Its Applications

There are many ways to communicate between the user and a product. One of the best ways is audio communication using a buzzer IC. So during the design process, understanding some technologies with configurations is very helpful. So, this article discusses an overview of an audio signaling device like a beeper or a buzzer and its working with applications.

What is a Buzzer?

An audio signaling device like a beeper or buzzer may be electromechanical or piezoelectric or mechanical type. The main function of this is to convert the signal from audio to sound. Generally, it is powered through DC voltage and used in timers, alarm devices, printers, alarms, computers, etc. Based on the various designs, it can generate different sounds like alarm, music, bell & siren.

Buzzer Pin Configuration

The **pin configuration of the buzzer** is shown below. It includes two pins namely positive and negative. The positive terminal of this is represented with the '+' symbol or a longer terminal. This terminal is powered through 6Volts whereas the negative terminal is represented with the '-'symbol or short terminal and it is connected to the GND terminal.

4.4 BLUETOOTH

Bluetooth is a wireless technology standard for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical radio bands, from 2.400 to 2.485 GHz, and building personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables. Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 30,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as **IEEE 802.15.1**, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks.[3] A manufacturer must meet Bluetooth SIG standards to market it as a Bluetooth device.[4] A network of patents apply to the technology, which are licensed to individual qualifying devices.

Name and logo

Name

The name *Bluetooth* is an Anglicised version of the Scandinavian *Blåtand*/*Blåtann* (Old Norse *blátǫnn*), the epithet of the tenth-century king Harald Bluetooth who united dissonant Danish tribes into a single kingdom. The implication is that Bluetooth unites communication protocols.[7]

The idea of this name was proposed in 1997 by Jim Kardach of Intel who developed a system that would allow mobile phones to

Received: 21-05-2026 | Accepted: 21-06-2026 | Published: 27-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

communicate with computers.[8] At the time of this proposal he was reading Frans G. Bengtsson's historical novel *The Long Ships* about Vikings and King Harald Bluetooth.[9][10]

Logo

The Bluetooth logo is a bind rune merging the Younger Futhark runes (ᚼ, Hagall) and (ᛒ, Bjarkan), Harald's initials.

V. METHODOLOGY & IMPLEMENTATIONS

MODULE SPLIT-UP

1. Biometric Acquisition Module

• Fingerprint, Facial

2. Authentication Processing Module

• Multi-modal verification logic

• Microcontroller-based decision-making

3. Secure Storage Module

• Encrypted template storage

• User database handling

4. Access Control Module

• Door lock control

• Alarm and tamper detection

5. Admin Interface Module

• Enrollment, deletion, logs

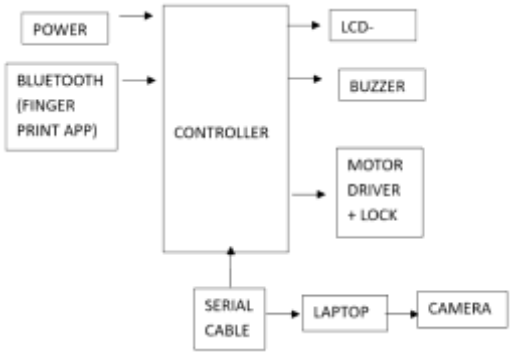
• System configuration

6. Notification Module

• Access indication

• Alert notifications (optional GSM)

BLOCK DIAGRAM



Working of Block Diagram

1. Power Supply

The power supply unit provides regulated DC voltage (5V/12V) to all components in the system.

- Ensures stable operation of the Arduino controller.
- Supplies required voltage to Bluetooth module, LCD, buzzer, and motor driver.
- Provides higher voltage (typically 12V) for the electromagnetic lock or motor.

Stable power is essential to avoid malfunction during authentication or lock operation.

2. Controller (Arduino – Central Processing Unit)

The controller acts as the brain of the system**.**

It performs the following tasks:

- Receives authentication data from Bluetooth (Fingerprint App).
- Processes fingerprint verification results.
- Communicates with laptop via serial cable.
- Controls LCD display messages.
- Activates buzzer for alerts.
- Sends signals to motor driver to lock/unlock door.

All decision-making and authentication logic are programmed inside the controller.

3. Bluetooth Module (Fingerprint App)

The Bluetooth module (HC-05/HC-06) connects wirelessly to a mobile application.

Working:

1. User opens the Fingerprint App on mobile.
2. User scans fingerprint using the mobile app.
3. App verifies fingerprint locally.
4. If verified, app sends authentication signal via Bluetooth to controller.
5. Controller receives signal and processes access request.

This acts as a second authentication layer (two-factor authentication).

Received: 21-05-2026 | Accepted: 21-06-2026 | Published: 27-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

4. Serial Cable – Laptop – Camera

The serial cable connects the controller to a laptop.

Working:

- Used during programming and system configuration.
- Laptop can monitor system logs.
- Camera (optional facial recognition module) may be connected to laptop.
- Camera captures user image for additional verification.
- Laptop processes image and sends authentication result to controller.

This setup can enable optional facial recognition as a third authentication factor.

5. LCD Display

The 16x2 LCD provides real-time system feedback such as:

- "System Ready"
- "Place Finger"
- "Bluetooth Connected"
- "Access Granted"
- "Access Denied"

This helps users and administrators understand system status.

6. Buzzer

The buzzer generates sound alerts:

- Short beep → Successful authentication.
- Long beep → Access denied.
- Continuous beep → Intrusion attempt detected.

It enhances security awareness.

7. Motor Driver + Lock Mechanism

The motor driver controls the electromagnetic lock or solenoid lock.

Working:

- If authentication is successful → Controller sends HIGH signal to motor driver.
- Motor driver activates lock mechanism.
- Door unlocks for predefined time (e.g., 5 seconds).
- After timeout → Door automatically locks again.

If authentication fails, the lock remains closed.

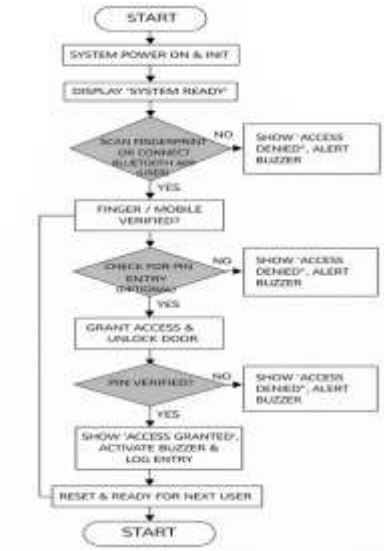
Step-by-Step Working Process

1. Power supply turns ON the system.
2. Controller initializes Bluetooth, LCD, and lock system.
3. LCD displays "System Ready."
4. User opens Fingerprint App and scans fingerprint.
5. App verifies fingerprint and sends signal via Bluetooth.
6. Controller receives authentication signal.
7. (Optional) Camera verification through laptop confirms identity.
8. Controller checks authentication conditions.
9. If verified:
    - LCD displays "Access Granted."
    - Buzzer gives short beep.
    - Motor driver unlocks door.
10. If not verified:

- LCD displays "Access Denied."
- Buzzer gives warning sound.
- Door remains locked.

11. System resets and waits for next user.

Flow Chart



Applications

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

1. Research Laboratories
   - Restrict access to authorized researchers only.
   - Protect sensitive experiments and confidential data.
   - Maintain secure entry logs for audit purposes.
2. Server Rooms & Data Centers
   - Prevent unauthorized access to critical IT infrastructure.
   - Reduce risks of data theft or sabotage.
   - Ensure multi-factor verification before entry.
3. Educational Institutions
   - Secure examination control rooms and administrative offices.
   - Restrict access to faculty rooms and laboratories.
   - Control hostel entry and exit monitoring.
4. Industrial Facilities
   - Limit entry to hazardous or restricted production areas.
   - Secure inventory storage and equipment rooms.
   - Monitor employee access in real time.
5. Government & Defense Buildings
   - Protect classified areas with multi-modal authentication.
   - Maintain secure access logs for compliance and auditing.
   - Ensure standalone operation without network dependency.
6. Residential Smart Homes
   - Provide biometric door unlocking for homeowners.
   - Replace traditional keys with fingerprint-based access.
   - Enhance family safety with Bluetooth and PIN verification.
7. Banks & Financial Institutions
   - Secure vault rooms and restricted cabins.
   - Enable multi-factor authentication for high-security zones.
8. Hostels & Apartments
   - Monitor entry of residents.
   - Prevent unauthorized access.
   - Provide secure access for authorized tenants only.
9. Healthcare Facilities
   - Restrict access to operation theatres and medicine storage rooms.
   - Protect patient records and sensitive medical data.
10. Corporate Offices
    - Control employee access to confidential departments.
    - Maintain attendance tracking and access history.

VI. CONCLUSION & FUTURE SCOPE

CONCLUSION

The Secure Pass system successfully demonstrates a reliable, intelligent, and highly secure standalone access control solution using multi-modal authentication. By integrating fingerprint verification, Bluetooth-based mobile authentication, and optional PIN validation within an Arduino-based embedded framework, the system significantly enhances identity verification accuracy and reduces unauthorized access risks. Unlike conventional lock-and-key mechanisms or single-factor authentication systems, Secure Pass provides multiple layers of security, making it far more resistant to duplication, spoofing, and credential sharing.

One of the major strengths of the system is its standalone architecture. It operates independently without relying on external servers or continuous internet connectivity. This ensures uninterrupted functionality even during network failures or cyber-attacks. Local encrypted storage of biometric templates enhances data privacy and minimizes the risk of centralized database breaches. The embedded controller processes authentication requests in real time, enabling fast decision-

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

making and minimal delay during access verification.

The inclusion of an LCD display and buzzer improves user interaction by providing clear visual and audible feedback. The motor driver and locking mechanism ensure secure physical access control, while optional logging and administrative features support audit trail maintenance. The system is energy-efficient, cost-effective, and suitable for various environments such as research laboratories, educational institutions, industrial facilities, and residential buildings.

Overall, Secure Pass addresses the limitations of traditional security systems by combining biometric intelligence, wireless communication, and embedded processing into a single, dependable platform. It offers enhanced security, improved reliability, and strong data protection while maintaining ease of use and scalability.

FUTURE SCOPE

Although Secure Pass provides a robust and efficient security solution, several enhancements can further improve its capabilities and adaptability to modern security requirements.

1. IoT and Cloud Integration

Future versions can integrate IoT-based monitoring dashboards for remote access management, centralized logging, and real-time notifications.

2. GSM Alert System

The system can be expanded to send SMS alerts to administrators in case of unauthorized access attempts or tampering.

3. Facial Recognition Integration

Adding a camera module with embedded facial recognition can introduce an additional biometric factor, further reducing spoofing risks.

4. AI-Based Behavioral Analysis

Artificial Intelligence algorithms can analyze user access patterns and detect suspicious behavior automatically.

5. Mobile App Enhancement

A dedicated secure mobile application can allow remote user management, temporary access granting, and activity monitoring.

REFERENCES

[1] Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.

[2] Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.

[3] Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against traffic tampering, MITM hash-rate hijacking, and template coercion. International Journal of Communication Networks and Information Security, 13(3), 718–728.

[4] Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.

[5] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465.

[6] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[7] Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[8] Kavuri, S. (2025). Critical Review of Software Testing Problems in the Current Decade. International Journal on Science and Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.9469.

[9] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. Computer Fraud and Security, 50–57. https://doi.org/10.52710/cfs.886.

[10] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875.

[11] Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329.

[12] Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. Journal of Computer Science and Technology Studies, 7(8), 1097-1104.

[13] Shashank, A. (2025). AI-Enhanced ETL Processes: Leveraging Artificial Intelligence for Optimized Data Integration Systems. Journal Of Multidisciplinary, 5(8), 219-225.

[14] Harshitha, G. K., Nandigama, C., & Thiripalu, P. (2026). An exploration into identification of opportunities and challenges of establishing and running an enterprise in the area of biofuels. Minnesota Journal of Business Law and Entrepreneurship, 2026(1), 1159–1168.

[15] Susarla, R. S., Boyapati, P. K., & Kandula, S. T. R. (2025, July). Cloud-Based Secure Data Storage in Smart Cities Using Central-Smoothing Hypergraph Neural Networks. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 279-284). IEEE.

[16] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219.

[17] Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783.

[18] Venkata Pavan Kumar Gummadi. (2025). MuleSoft Architectural Paradigms and Sustainability: A Comprehensive Technical Analysis. Journal of Computer Science and Technology Studies, 7(12), 534–540. https://doi.org/10.32996/jcsts.2025.7.12.59.

[19] Gummadi, V. P. K. (Ed.). (2025). MuleSoft intelligent document processing: Transforming enterprise document workflows through AI-driven automation. Journal of Computational Analysis and Applications, 34(12). https://doi.org/10.48047/jocaaa.2025.34.12.16.

[20] Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Service Level Objective (SLO) Observability with Splunk and Dynatrace in Microservices. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541542.

[21] Pokala, H. K., & Gummadi, V. P. K. (2026). Autonomous AI-Powered Resource Management for Apache Flink on Amazon EKS. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541881.

[22] Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Securing APIs in Government Clouds and Runtime Fabric Using FIPS-Enabled MuleSoft. 2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–6. https://doi.org/10.1109/icaiset66439.2026.11542099.

[23] Kumar Gummadi, V. P., Chilamkurthi, L. S., & Kavuri, S. (2026). Distributed Platform Architecture and API-Led Integration. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–6. https://doi.org/10.1109/icaiset66439.2026.11541787.

[24] Gajula, S. (2025). Cloud transformation in financial services: A strategic framework for hybrid adoption and business continuity. International Journal of Scientific Research in Computer Science, Engineering and Information technology.

[25] Gajula, S., Bondhala, S., & Margam, M. (2026). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–7. https://doi.org/10.1109/icaic67076.2026.11395835.