IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

SafeNest: A Multilayered IOT Security System for Smart Homes

Sakshi Doke[1], Shivani Borhade[2], Dipti Mule[3] , Prof. Pallavi Gholap[4]
Students, Department of AI&DS Engineering[1,2,3]
Professor, Department of AI&DS Engineering[4]
Jaihind College of Engineering Kuran, Maharashtra, India.

Abstract: *This paper proposes a high level IoT-based house security framework involving three unmistakable modules intended to improve generally security. The main module utilizes RFID innovation for door mechanization, where vehicles outfitted with RFID cards are perceived by anEM18 module, permitting consistent, secure admittance to approved vehicles. This computerized framework wipes out the requirement for manual entryway control and guarantees that as it were enrolled vehicles can enter the premises. The subsequent module centers around a home storage, which is gotten through a three-way confirmation process that incorporates unique finger impression acknowledgment, RFID filtering, and a mystery key entered by means of a keypad. This complex way to deal with storage security guarantees that entrance is conceded just when each of the three confirmation factors are effectively given, incredibly decreasing the gamble of unapproved access. The third module improves border security by utilizing a movement sensor to distinguish unapproved development at the rear of the house. After recognizing movement, the framework right away sends an alarm to the property holder's cell phone, empowering ideal reactions to possible dangers. This IoT based framework incorporates RFID innovation, multifaceted verification, and constant portable cautions to give a extensive and powerful security answer for private settings*

Keywords: IoT-based security system, RFID technology, Gate automation, Home locker security, Multi-factor authentication, Fingerprint recognition, Motion sensor, Real-time alerts

I. INTRODUCTION

This paper proposes a high level IoT-based house security framework involving three unmistakable modules intended to improve by and large wellbeing [1][4][6]. The first module utilizes RFID innovation for door robotization, where vehicles outfitted with RFID cards are perceived by an EM18 module, permitting consistent, secure admittance to approved vehicles [7][17]. This computerized framework wipes out the requirement for manual door control and guarantees that main enlisted vehicles can enter the premises [7][9].The resulting module bases on a home stockpiling, which is gotten past a three way affirmation process that consolidates finger impression affirmation, RFID separating, and a secret key entered through a keypad [7][9]. This complicated method for managing stockpiling security ensures that entry is yielded when each of the three check factors are actually given, tremendously reducing the bet of unapproved access [9]. The third module updates line security by using a development sensor to recognize unapproved improvement at the back of the house[6]. Later recognizing development, the system. instantly sends a watchfulness to the home loan holder's phone, enabling ideal responses to expected risks [6].

II. PROBLEM STATEMENT

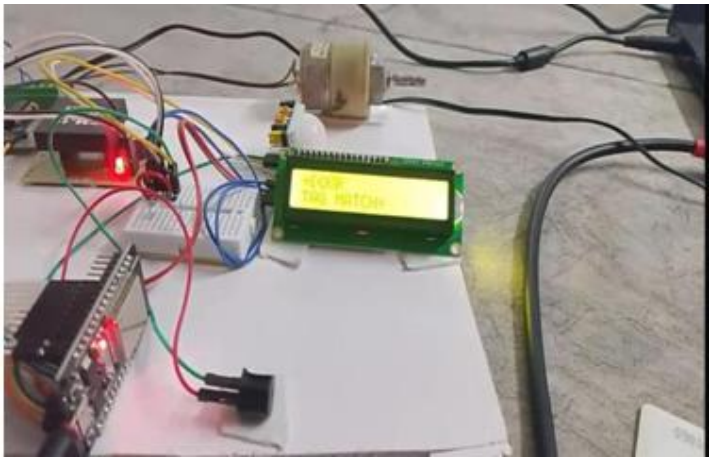
To Develop Multilayered Iotbased House Security System With Rfid Gate Control,Threeway Locker Authentication, And Motiontriggered Theft Detection.

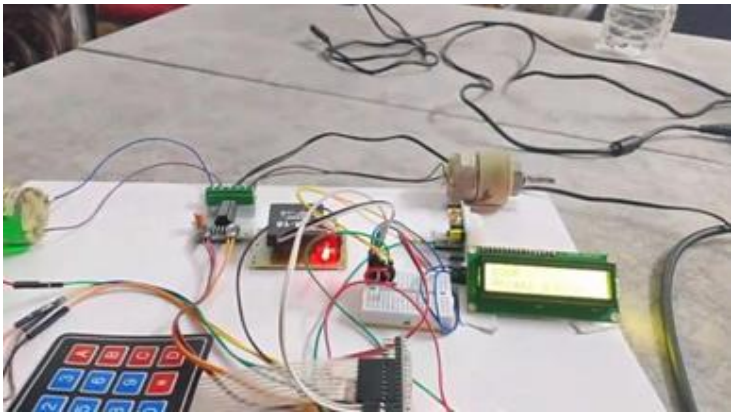
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

III. PROPOSED SYSTEM

The proposed system is a microcontroller-based electronic access control mechanism that combines password authentication and optional RFID verification for secure entry. It utilizes a 4x4 keypad to input a numeric password, which is then processed by a microcontroller (such as an Arduino or similar development board). An LCD display provides real-time feedback to the user, such as prompting for password entry or indicating access status. Upon entering the correct password, the system activates a relay module to power a DC motor or solenoid, simulating the unlocking of a door or mechanism. Additionally, an RFID module is integrated into the system to allow access using RFID cards, offering an alternative or dual-layer verification method. This system is designed for applications such as digital door locks, secure lockers, and access-controlled areas in residential, commercial, or institutional environments, emphasizing both security and user convenience.

IV. RESULT





V. SYSTEM ARCHITECTURE

The system architecture is centered around a microcontroller that acts as the main control unit. It receives inputs from two sources: a 4x4 matrix keypad for password entry and an RFID module for card-based authentication. Upon receiving input, the microcontroller processes the data and checks it against stored credentials. If the input is valid, the microcontroller sends a signal to the relay module, which in turn controls a DC motor or solenoid lock to unlock the door. An LCD display is used to provide real-time feedback to the user, such as instructions, error messages, or confirmation of access. Power is supplied via a USB cable or external adapter.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

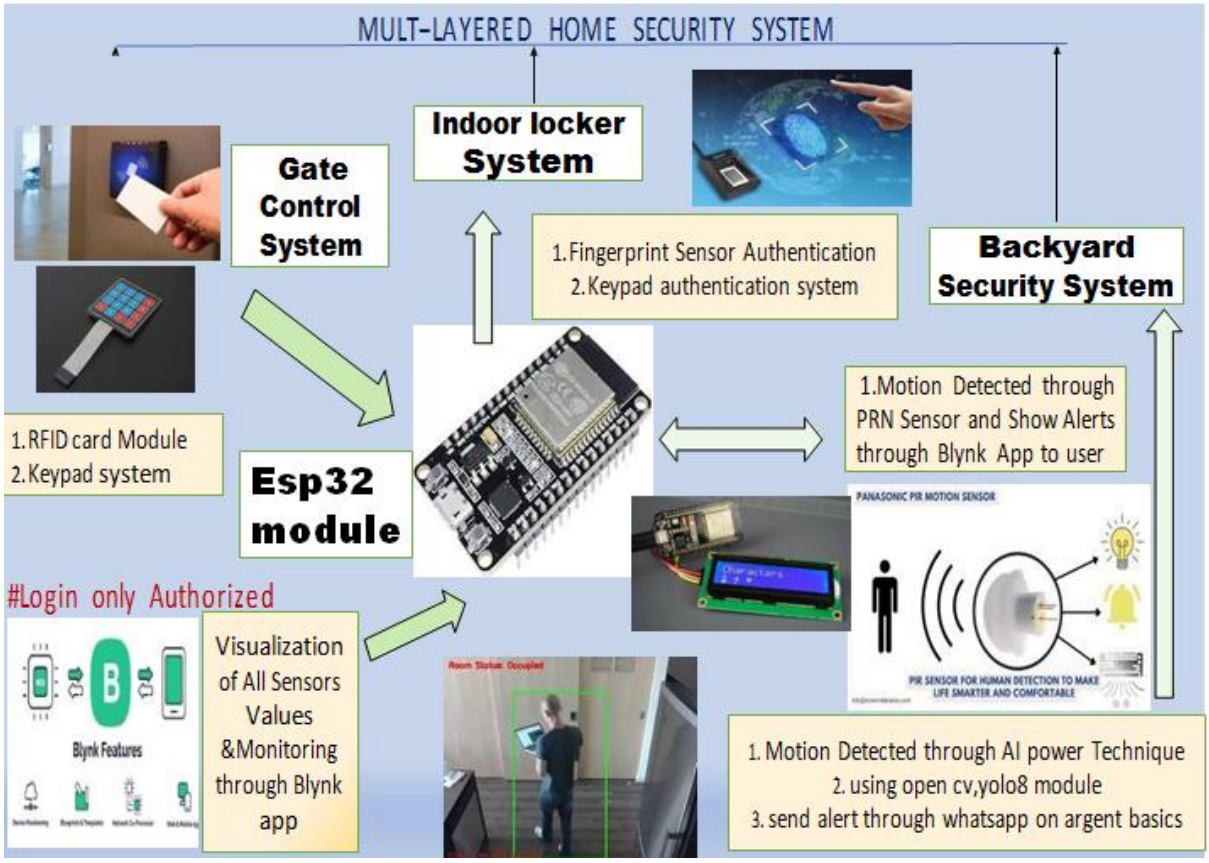


Figure : Architecture diagram

VI. LITERATURE REVIEW

Samrah Arif,et.al, "Investigating Smart Home Security: Is Blockchain the Answer? ", doi:10.1109/ACCESS.2020.3004662(2024)[1]

Investigating Smart Home Security: Is Blockchain the Answer?" explores the potential of blockchain technology to enhance security in smart home systems. It examine show blockchain's decentralized, tamper-resistant nature could address vulnerabilities in IoT devices, ensure data integrity, and improve privacy, while considering challenges like scalability and implementation costs. The investigation aims to determine if blockchain can provide a more robust and secure foundation for the future of smart home security

K.Sachine,et.al, "SMART HOME SECURITY SYSTEM USING IOT", doi:10.1109/ICCCNT 56998.2023.10307277(2023)[2]

A Smart Home Security System using IoT integrates various interconnected devices and sensors to enhance home safety and monitoring. This system typically includes cameras, motion detectors, door/window sensors, and alarms, all of which communicate via a centralized hub or cloud platform. Utilizing IoT technology allows for real-time data collection and remote access, enabling homeowners to monitor their property from anywhere through mobile applications. The system can also leverage machine learning algorithms to identify unusual patterns and send alerts to users. Additionally, the integration of smart assistants enhances usability and control. Overall, this approach not only improves security but also offers convenience and peace of mind for users

Naba. M.Allifah,et.al "Ranking Security of IoT-Based Smart Home Consumer Devices." doi:10.1109/ACCESS.2022.3148140(2022)[3]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

The security of IoT-based smart home consumer devices is a critical concern, as these devices often collect and transmit sensitive personal data. The security landscape varies significantly across different products, influenced by factors such as manufacturer practices, software updates, and the underlying protocols used for communication. Many devices are vulnerable to threats like unauthorized access, data breaches, and malicious attacks due to inadequate encryption and authentication mechanisms. Effective security measures should include robust encryption, regular firmware updates, and user awareness about privacy settings. As the adoption of smart home technology grows, ensuring strong Security protocols is essential to protect users from potential cyber threats

Qusay I.Sarhan,et.al, "Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform.",doi:10.1109/ACCESS. 2020.3008610(2020)[4]

A systematic survey on smart home safety and security systems using the Arduino platform would review various implementations and advancements in smart home technology focused on enhancing security. It would explore how the open-source Arduino platform is used to develop cost-effective, customizable, and user-friendly systems. These systems can include sensors for detecting intrusions, smoke, fire, and gas leaks, as well as cameras and alarms for monitoring. The survey would analyze different Arduino-based projects, highlighting their architectures, communication protocols (like Wi-Fi, Zigbee, or Bluetooth), and effectiveness in real-world applications. It would also consider challenges such as power consumption, integration with IoT, and scalability

Arun Cyril Jose,et.al, "Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home",doi:10.1109/ACCESS. 2016.2606478(2016)[11]

Integrating device fingerprinting into smart home systems enhances security by uniquely identifying and authenticating each device connected to the network. This technology analyzes various attributes of devices, such as hardware specifications, software versions, and network behavior, creating a distinct profile for each device.By employing device fingerprinting, smart homes can detect unauthorized devices attempting to access the network and differentiate between legitimate and potentially malicious devices. This proactive approach minimizes risks of unauthorized access and enhances the overall integrity .

VII. OBJECTIVE

The user interacts with a 4x4 keypad to input a code, which is processed by a microcontroller such as an Arduino. The microcontroller also communicates with an LCD display to provide user feedback and an RFID reader to authenticate access cards. Upon successful authentication through the keypad or RFID reader, the microcontroller activates a relay module that controls a DC motor or solenoid, which functions as the door lock mechanism. The entire system is powered through a USB connection or an external adapter.

VIII. METHODOLOGY

Algorithm

The system's workflow is broken down into four key steps, as outlined below:

1. Smart Home Security System (Central Module)

Acts as the central hub, managing all subsystems and connecting to the database.

2. Gate Control System

Uses RFID technology to control gate access.

Process:

RFID tag is scanned.

If data matches, the gate opens. If not, the gate remains closed.

3. Locker Access System

Features three-factor authentication mechanism:

Fingerprint scan. RFID card validation. PIN code entry.

Process:

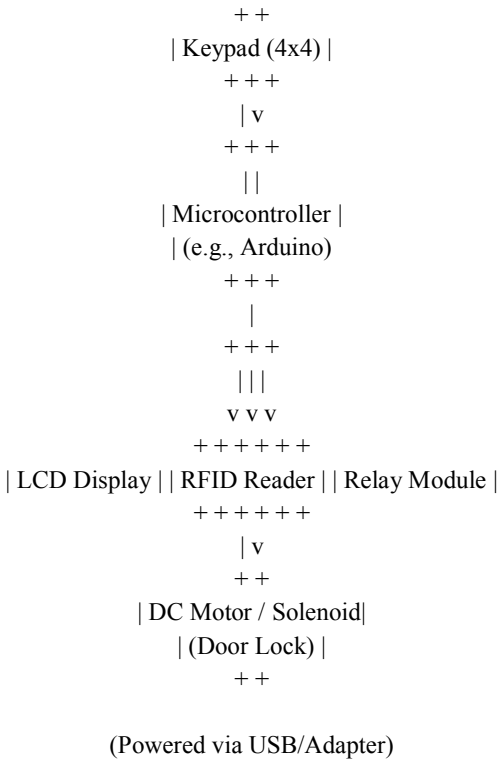
All credentials must match to grant access. Otherwise, access is denied.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

4. Motion Detection and Alert System
Sensors detect suspicious motion or activity around the secured area.
Process:
If suspicious activity is detected, an alert is sent. Data is logged in the database for review

5. Database
Stores data related to:
RFID tags.
User fingerprints.
Access logs and alerts.
Suspicious activity records for monitoring and analysis.

Workflow
1. Authentication Process:
- The gate and locker systems validate user credentials using RFID, fingerprints, and PIN codes.
- Verified actions are logged in the database.
2. Surveillance and Alerts:
- Motion detection identifies potential intrusions.



IX. CONCLUSION

All in all, the high level IoT-based house security framework offers a far reaching, present day answer for the developing requirement for upgraded private security. By coordinating RFID innovation for door mechanization, multifaceted verification for home storage spaces, and continuous cautions through movement sensors, the framework gives a powerful security system that limits chances and amplifies comfort. Its measured and versatile plan guarantees it

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

very well may be custom fitted to meet assorted security needs, from individual homes to bigger networks and organizations. The utilization of IoT advancements takes into account realtime checking, controller, and mechanization, giving property holders inner serenity through day in and day out security. The framework further develops security as well as likewise smoothes out ordinary activities, offering costeffective, easy to use arrangements that diminish the requirement for manual oversight or security faculty. In a period of expanding security concerns and the ascent of savvy homes, this IoT-based framework presents a ground breaking, dependable way to deal with defending homes, assets, and friends and family

X. FUTURE SCOPE

The Password and RFID-Based Door Lock System has strong future potential through integration with IoT for remote control, real-time alerts, and centralized access management. Enhancements like biometric authentication, mobile app support, voice assistant control, and power backup can greatly improve security, usability, and scalability. These upgrades position the system as a key component in modern smart home and building security solutions.

REFERENCES

[1]K.Sachine,et.al, ”SMART HOME SECURITY SYSTEM USING IOT”,doi:10.1109/ICCCNT 56998.2023.10307277(2023)
[2] Hanan F Alqahtani,et.al, ”Automated smart locker for college”,doi:10.1109/ICCAI S48893.2020.9096868(2023)
[3] Andi Pramono,et.al, ”Fingerprint-based Security System in Smart Portable Display at Brawijaya Museum.”, doi:10.1109/CITSM56380.2022.9935878(2022)
[4] NABA M.ALLIFAH,et.al, “Ranking Security of IoTBased Smart Home Consumer Devices”,doi:r 10.1109/ACCESS.2022.3148140(2022)
[5] ARUN CYRIL JOSE1,et.al, “Improving Home Automation Security Integrating Device Fingerprinting IntoSmartHome”,doi:10.1109/ACCESS.2022.2606478(2022)
[6] Aswin Jojo, “Intruder Detection System using IoT with Adaptive Face Monitoring and Motion Sensing Algorithm” (2022)
[7] Ahmad Anwar Zainuddin, “Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology”doi:https://doi.org/10.56532/mjsat. (2022)
[8] Yazan Alshboul,”Cybersecurity of Smart Home Systems: Sensor Identity Protection”(2021)
[9] Rohit Tripathi “Intelligent Physical Access Control System Through Three-Stage Verification Using IoT”(2021)
[10] Qusay I.Sarhan,et.al, ”Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform.”,doi:10.1109/ACCESS.2020.3008610(2020)
[11] S. Siboni,et.al, “Security ranking of IoT devices usinganAHPmodel”,doi:10.1007/97830.30497.859(2020
[12]Andreas Kamilaris,et.al, “Enabling smart homes using webt echnologies”,doi:https://doi.org/10.1063/5.00 32939(2020)
[13] Amit verma, “A Multi Layer Bank Security System” DOI:10.1109/ICGCE.2013.6823565(2020)
[14] AKM Jahangir Alam Majumder and Joshua Aaron Izaguirre,”A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition”DOI:10.1109/COMPSAC48688.2020.0-132(2020)
[15] Yinxin Wan,“A Multi-Layer Security Monitoring System for Internetof-Things in Smart Homes”(2020)