# BLOCKCHAIN-ENABLED SECURITY LOCK SYSTEM US ING IOT

Suma Christal Mary Sundararajan [1], BR ASHWINKUMAR [2,3], SHRI HARRI PRIYA , R [1], and GIRIKISHORE B [1]

[1]Affiliation not available
[2]animalar Institute of Technology,Sri Sairam Institute of Technology
[3]panimalar Institute of Technology,Sri Sairam Institute of Technology

October 31, 2023

**Abstract**

In recent times, digital locks have become increasingly popular for securing homes and valuables. However, these locks can still be vulnerable to picking or disabling by those with the necessary skills or tools. To address this issue, this project proposes the use of blockchain technology and biometrics or smartphones to create a more secure system for home security. By leveraging the decentralized and tamper-proof nature of blockchain, combined with biometric identification or smartphone authentication and using the power of IOT technology, homeowners can ensure that their property remains secure and protected from unauthorized access. This project offers a novel solution to the problem of digital lock vulnerabilities, with potential applications in the fields of home security and asset protection.

# BLOCKCHAIN-ENABLED SECURITY LOCK SYSTEM USING IOT

**[1]DR.S. SUMA CHRISTAL MARY, [2]B.R. ASHWINKUMAR, [3]R. SHRI HARRI PRIYA, [4]B.GIRIKISHORE**

*[1]Professor and Head of Department of I.T, Panimalar Institute of Technology, Anna University, Chennai, India.sumasheyalin@gmail.com*
*[2]Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India, ashwinkumarbr27@gmail.com.*
*[3]Student, Department of Computer Science and Engineering, Sri Sai Ram Institute of Technology,Chennai, India. ,rshriharripriya19@gmail.com*
*[4]Student, Department of Computer Science and Engineering, Sri Sai Ram Institute of Technology, Chennai, India.,girikishorebabu@gmail.com*

***Abstract*— In recent times, digital locks have become increasingly popular for securing homes and valuables. However, these locks can still be vulnerable to picking or disabling by those with the necessary skills or tools. To address this issue, this project proposes the use of blockchain technology and biometrics or smartphones to create a more secure system for home security. By leveraging the decentralized and tamper-proof nature of blockchain, combined with biometric identification or smartphone authentication and using the power of IOT technology, homeowners can ensure that their property remains secure and protected from unauthorized access. This project offers a novel solution to the problem of digital lock vulnerabilities, with potential applications in the fields of home security and asset protection.**

***Keywords: blockchain, home security, IOT Technology, Biometric system, decentralized.***

## I.INTRODUCTION: -

In recent years, there has been a growing interest in developing more secure and dependable systems for home security and access management. With the introduction of the Internet of Things (IoT) and blockchain technology, there has been an increasing focus on exploring innovative solutions that integrate these two technologies to create more robust and reliable systems.

This project proposes the implementation of an IoT-based, blockchain-enabled security lock system that combines the connectivity and practicality of IoT devices with the security and decentralization of blockchain. This system offers a more reliable and secure solution for access control and monitoring, with potential applications in areas such as home security, asset protection, and smart buildings.

The use of IoT devices in this security lock system enables homeowners to remotely control and monitor access to their homes, without having to be physically present. For example, homeowners can use their smartphones to unlock or lock doors, grant access to visitors, or monitor activity in their homes. This level of convenience and connectivity is a major advantage of using an IoT-based security lock system.

The use of blockchain technology further enhances the security of the system by providing a tamper-proof and decentralized record of access activity. This ensures that any attempts to modify or tamper with access records are immediately detected, making it more difficult for hackers or intruders to gain unauthorized access to homes or assets.

However, deploying a blockchain-enabled security lock system utilizing IoT can also pose certain challenges. For example, there may be concerns about the scalability of the system, as the number of devices and users increases. There may also be challenges around data privacy and security, as the system collects and stores sensitive personal data.

Overall, this project offers an innovative solution to the challenges of home security and access management, by leveraging the strengths of IoT and blockchain technology. By addressing the challenges of scalability and data privacy, this system has the potential to enhance the security and reliability of access control and monitoring, with potential applications in a wide range of settings.

## II.RELATED WORK: -

### *A. IoT Enhanced Smart Door Locking System:-*

The proposed approach addresses the security aspect of smart home technologies by developing a door lock system that can be controlled using a Smartphone-connected, Bluetooth-enabled system using an Arduino UNO microcontroller. The system allows homeowners to monitor their homes remotely and provides them with an added layer of security by enabling them to control access to their homes.

To use the system, users must first install the developed Android application on their devices, such as smartphones, laptops, or tablets, and log in using their login credentials, such as a username and password. These credentials are verified in a database over the internet, and if they are valid, the user can open or close the door lock remotely.

If the credentials are invalid, the system will trigger an alarm in the form of a buzzer and send an SMS alert to the owner of the building. This feature provides an added level of security in the event of attempted unauthorized access.

This approach can be scaled up to commercial sectors like ATMs and vending machines by using other wireless communication methods, such as Wi-Fi or cellular networks. This can further enhance the security of these systems by enabling real-time monitoring and control.

Overall, the proposed approach demonstrates the potential of using IoT and smart home technologies to enhance security in homes and commercial settings. By leveraging the power of Bluetooth-enabled microcontrollers, wireless communication, and database management systems, this approach provides homeowners and business owners with a scalable, secure, and easy-to-use system for controlling access to their properties.

### *B. Wireless Biometric Lock Using Arduino with the IoT: -*

The importance of smart home security cannot be overstated, as it plays a crucial role in enhancing home safety. The aim of this project is to create a Bluetooth-

based system that allows users to remotely control their door locks using a mobile device or tablet. This innovative system enables users to lock and unlock their doors from inside or outside their homes using a Bluetooth-enabled device.

The primary objective of this project is to provide a convenient and efficient solution for users to access their homes. For example, if the user forgets to lock the door on the primary floor or any other floor, they can easily lock it from their mobile device or PC, saving time and energy.

The system comprises of the latest Arduino board, a solenoid lock or servo motor, and a Bluetooth module that uses standard protocols for wireless communication. These components work seamlessly together to ensure that the door can be locked and unlocked with ease using a Bluetooth-enabled device. The use of an Arduino board allows for easy programming and control of the system, making it user-friendly. The solenoid lock or servo motor ensures that the door is securely locked and unlocked, thereby enhancing home security. Additionally, the Bluetooth module uses standard protocols for wireless communication, ensuring seamless and reliable communication between the mobile device and the door lock system.

### C. *Internet of Things (IoT) Based Door Lock Security System: -*

Doors are an essential part of a building, allowing entry without damaging walls while providing privacy, security, and environmental control. However, biometric systems can sometimes fail to detect fingerprints due to factors such as sweat, and people often lose their keys or forget their pin numbers for door locks. This paper aims to introduce a door lock security system that uses Arduino and a mobile app to detect the intensity of a secret knock and transmit it wirelessly to unlock or lock the door. This innovative solution provides a reliable and convenient alternative to traditional access control methods.

### *D. Integrated Smart House Security System Using Sensors and RFID: -*

Efficiency, effectiveness, and energy conservation have captured the attention of many researchers. This study focuses on the automation of door locks and lighting systems in a security system. The Arduino Uno microcontroller serves as the central control unit for the system. The microcontroller uses various sensors, including Radio Frequency Identification (RFID), Keypad 4×4, Limit Switch, Light Dependent Resistance (LDR), and Passive Infra-Red (PIR), to secure the door. When these sensors detect an output, the microcontroller responds by controlling the Solenoid, Buzzer, Liquid Crystal Display (LCD) display, and lamp. The door unlocks if the RFID and Keypad 4×4 passwords are correct, with a maximum read range of 2 cm between the tag and reader. If the Limit Switch detects an open door without proper identification, the buzzer sounds. The lamp turns on automatically when conditions are dark and there is human movement in the room, as measured by the PIR sensor and LDR. The maximum range of the PIR sensor is 4 meters, as confirmed by testing.

## III.PROPOSED SYSTEM: -

### Blockchain Algorithm -

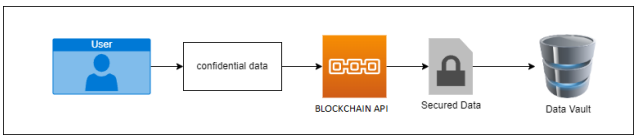



Fig 1. Blockchain workflow

When a user registers their device or lock system, the data they provide is converted into individual blocks. Each block is connected to the previous block in a chain-like structure, which creates a blockchain.

Before the user's data is added to the blockchain, it goes through a hashing process using the MD5 hash creator algorithm. This algorithm generates a unique and fixed-length string of characters, which represents the user's data in a secure and tamper-resistant format.

Once the user's data has been hashed, it is then sent to the blockchain API, which creates a secure block that stores the user's data. The blockchain API creates a new block with the user's hashed data and adds it to the blockchain. The new block is then connected to the previous block, creating a chain.

The blockchain API ensures that each block is encrypted and tamper-proof, making it impossible for anyone to change the data stored within it without being detected. This creates a secure and reliable way to store user data.

The blockchain itself is stored in a semi-decentralized data vault, which is managed by a network of nodes. This ensures that the data is always available, even if one of the nodes fails or is compromised.

Overall, using a blockchain to store user data provides a secure and tamper-proof way to store information, which is especially important for sensitive data like that used in lock systems or other security devices. The use of a semi-decentralized data vault further ensures the availability and reliability of the data, making it a robust and reliable storage solution.

### A. LOCK REGISTERATION

The process of registering a lock system involves assigning a unique product id to the device. This product id will serve as an address key during the

authentication process when a user tries to access the lock system through their mobile device. The product id acts as a unique identifier for the lock system, ensuring that the authentication process is secure and reliable.
To ensure that the lock system is pre-registered with a hash code, a cryptographic algorithm is used to generate a unique and permanent address for the device. This hash code is stored securely and cannot be changed or modified by anyone, making it a reliable and trustworthy identifier for the lock system.

When a user registers for the lock system, they will provide a code to permanently pair their primary device with the lock system. This code is unique to the user and ensures that only the registered device can access the lock system. The code is securely stored on both the lock system and the user's mobile device, ensuring that the authentication process is reliable and secure.

Overall, the registration process for a lock system involves assigning a unique product id to the device, generating a hash code as a permanent address for the lock system, and allowing users to register their primary device by providing a unique pairing code. These steps ensure that the authentication process is secure, reliable, and trustworthy.

### B. USER REGISTRATION

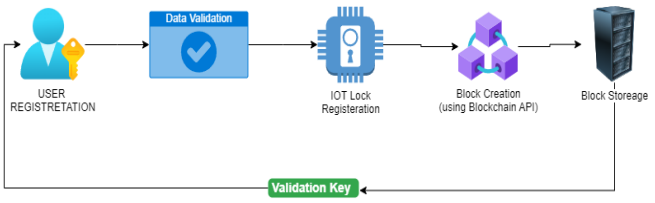



Fig 2. User registration workflow

During the registration process for the IoT lock system, the user will fill in all the necessary details. This typically includes basic personal information such as name, address, email, and phone number. Additionally, the user will enter the product key for the IoT lock system. This product key is a unique identifier that is permanently associated with the lock system and ensures that the user's lock system is authenticated and authorized.

Once the user has completed the registration process, they will be designated as the admin user for the lock system. As an admin user, they will have special privileges, including the ability to add family members and other authorized individuals who are allowed to enter the premises.

To add family members or other authorized users, the admin user will typically need to provide their basic personal information, including name and email address. The admin user may also be able to set specific access privileges for each user, such as limiting access to certain times or days of the week.

Overall, the registration process for an IoT lock system involves entering the product key for the lock system and registering as the admin user. As the admin user, the individual has the ability to manage and add other authorized users to the lock system. This ensures that access to the premises is secure and controlled, and only authorized individuals are allowed entry.

In an IoT lock system, the admin user has the ability to manage and control access to the lock system. This includes providing access to family members and guests.

Once a family member has been added to the lock system, the admin user will typically provide them with an access pin. This pin is a unique code that is used to unlock the lock system and gain access to the premises. Each family member may have their own unique pin, which can be used to track access and ensure that only authorized individuals are entering the premises.

In addition to providing access to family members, the admin user may also need to provide temporary access to guests. To do this, the admin user can generate a temporary key that is valid for a limited period of time. This temporary key can be shared with the guest, allowing them to unlock the lock system and gain access to the premises for a specified period of time. Once the temporary key expires, it becomes invalid and the guest can no longer access the premises.

Overall, the ability to manage access to the lock system is an important feature of an IoT lock system. By providing access pins to family members and generating temporary keys for guests, the admin user can ensure that only authorized individuals are able to enter the premises, while also maintaining a high level of security and control.

### C. IOT LOCK AUTHENTICATION

When using an IoT lock system with a mobile app, the authentication process typically begins with the user logging into the app using their username and password. This ensures that only authorized users are able to access the lock system and control the lock.

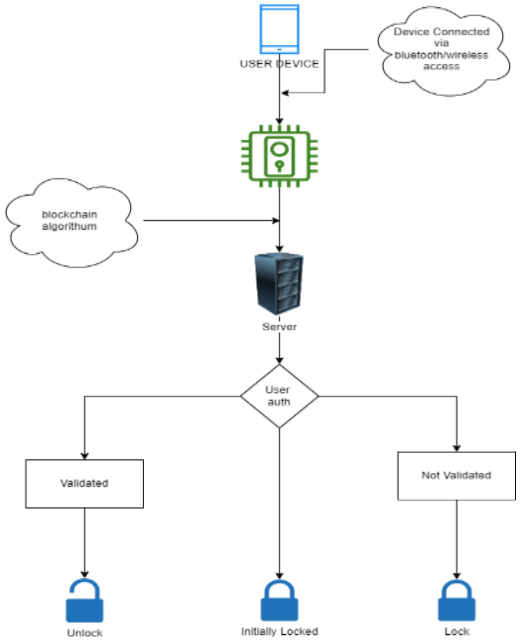



Fig 3. Authentication workflow

Once the user is logged in, they can access the lock controller page within the app. The app will typically indicate whether the lock system is connected or not. If the lock system is not connected, the user may need to follow specific steps to connect the app to the lock system.

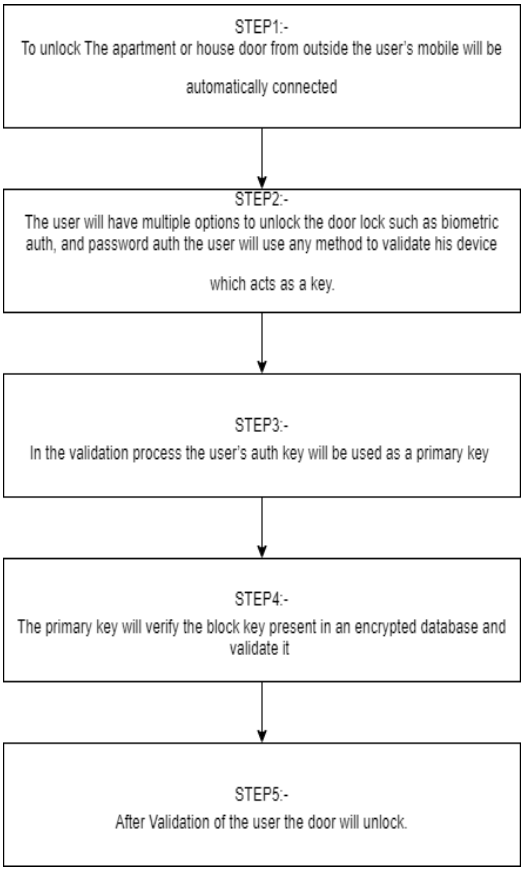
However, in some cases, the app may automatically connect to the lock system by default, so the user doesn't have to manually connect every time they use the app. This can make the authentication process more convenient and efficient for the user.

Once the app is connected to the lock system, the user can use the app to unlock the lock and gain access to the premises. To do this, the user typically needs to provide a six-digit pin, which is used to authenticate the user and ensure that only authorized individuals are able to unlock the lock.

Once the pin has been entered and verified, the lock will unlock, allowing the user to enter the premises. The app may also provide additional features, such as the ability to set specific access privileges for family members or guests, or to generate temporary access keys for guests.

Overall, the authentication process for an IoT lock system using a mobile app typically involves logging into the app, connecting to the lock system, and entering a six-digit pin to unlock the lock and gain access to the premises. This process is designed to be secure, convenient, and easy to use for authorized users.

## IV.ALGORITHM




## V.IMPLEMENTATION OF THE PROPOSED SYSTEM

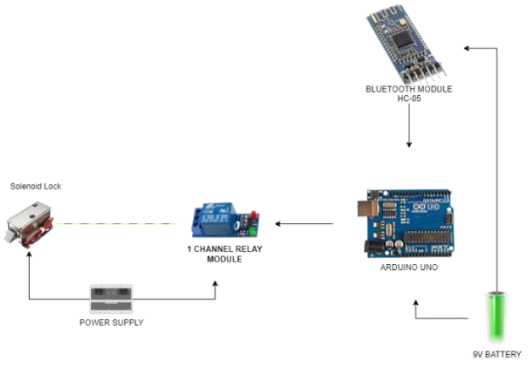



Fig 4. Hardware Implementation Diagram

The hardware used for the prototype are Arduino Uno, Solenoid Lock, 1-Channel Relay Module and Bluetooth Module HC-05.

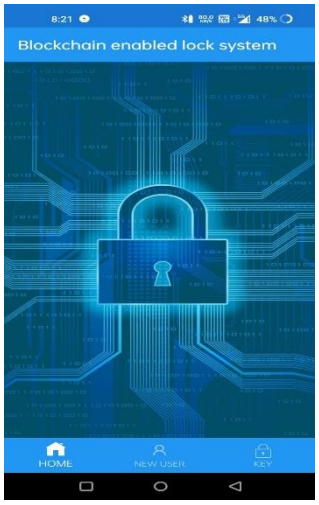



Fig 5. Prototype Screenshot: Home Page

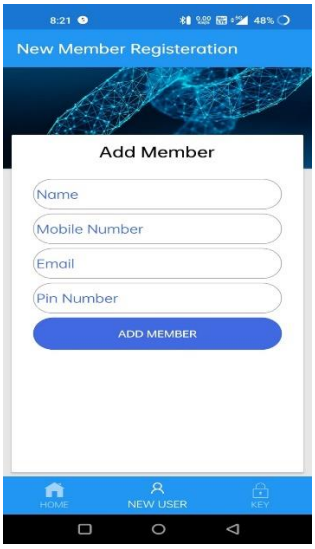



Fig 6. Prototype Screenshot: Registration Page


Fig 7. Prototype Screenshot: Control Page

Fig 8. Decentralized Encrypted Database

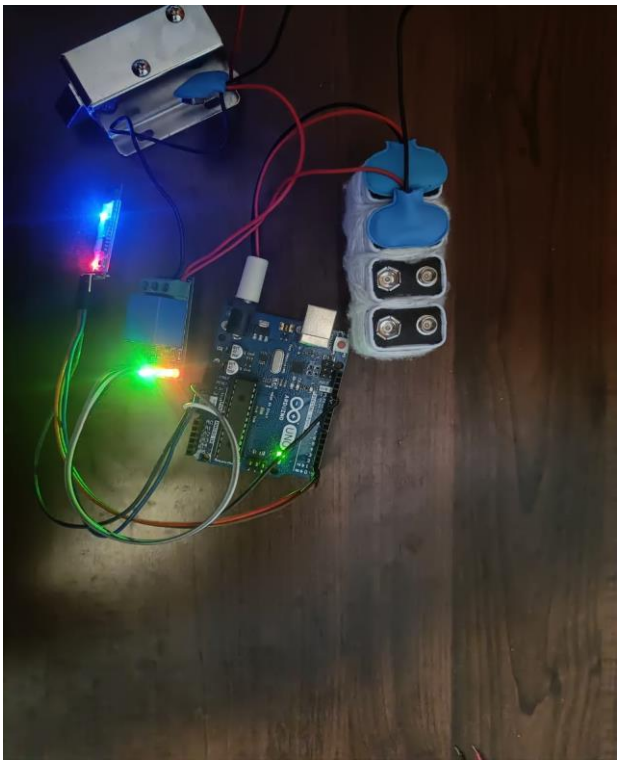


Fig 9. Hardware Design

In the above image Arduino uno is connected to a 9v battery for power supply.
For communication between the lock system and user device is connected via Bluetooth module.
1-Channel Relay Module is connected with the ground and 3.3v socket and the ground of Arduino and the other end is connected with the solenoid lock(12v) that completes the circuit.

## VI. FUTURE ENHANCEMENTS

There are several potential future enhancements that could be made to a blockchain-enabled security lock system using IoT, including:

1. Integration with Smart Home Systems: A blockchain-enabled security lock system can be integrated with other smart home systems, such as smart thermostats, smart lighting, and home security cameras. This integration can allow for seamless control of various home devices, enhancing the overall user experience and convenience.

2. Voice and Facial Recognition: Integration of voice and facial recognition technology can be incorporated into the blockchain-enabled security lock system to provide an extra layer of security. This can further prevent unauthorized access to the home.

3. Enhanced Data Privacy: As blockchain technology is tamper-proof and decentralized, it can provide enhanced data privacy and security. Future enhancements could be made to incorporate

additional layers of encryption to further protect sensitive data.

4. Remote Monitoring and Management: The blockchain-enabled security lock system can be enhanced to allow for remote monitoring and management. This feature can be beneficial for homeowners who are away from their homes and need to grant access to authorized individuals.

5. Multi-Factor Authentication: Multi-factor authentication can be incorporated into the blockchain-enabled security lock system, requiring multiple authentication methods, such as biometric identification and passcodes, to unlock the door. This can provide additional security against unauthorized access.

## VII.COMPARISON TABLE

| TECHNOLOGY | VULNERABILITIES |
|---|---|
| Biometric Devices | Risk of identity theft |
| RFID | Susceptible to relay and man-in-the-middle attacks |
| API | Susceptible to URL-based attacks |

**Table 1**

The proposed solution prevents the possibility of URL-based attacks by encoding the data sent via Blockchain API.

## VIII.CONCLUSION

In conclusion, the proposed use of blockchain technology and biometrics or smartphones for home security offers a promising solution to the vulnerabilities of traditional digital locks. By using the tamper-proof and decentralized nature of blockchain, combined with biometric identification or smartphone authentication, homeowners can ensure a more secure and reliable system for protecting their property from unauthorized access. The implementation of IoT technology can further enhance the security and convenience of the system. This project offers a novel approach to home security, with potential applications in asset protection and other fields where secure access control is required.

## IX.REFERENCES


1. Integrated Smart House Security System Using Sensors and RFID,
   Publisher: IEEE,
   https://ieeexplore.ieee.org/document/8527803
2. Wireless Biometric Lock Using Arduino with the IoT,
   Publisher: IEEE,
   https://ieeexplore.ieee.org/document/9760583
3. Internet of Things (IoT) Based Door Lock Security System,
   Publisher: IEEE,
   https://ieeexplore.ieee.org/document/9537052
4. IoT Enhanced Smart Door Locking System,
   Publisher: IEEE,
   https://ieeexplore.ieee.org/abstract/document/9214288
5. Enterprise API Security and GDPR Compliance: Design and Implementation Perspective
   Publisher: IEEE,
   https://ieeexplore.ieee.org/document/9194432
6. RFID Security and Privacy: A Research Survey
   Publisher: IEEE,
   https://ieeexplore.ieee.org/document/1589116
7. Challenges and opportunities in biometric security: A survey
   Publisher: Taylor and Francis Online,
   https://doi.org/10.1080/19393555.2021.1873464
8. Identifying users from the interaction with door handle
   Publisher: ScienceDirect,
   https://doi.org/10.1016/j.pmcj.2020.101293
9. Digital door-lock using authentication code based on ANN encryption
   Publisher: ScienceDirect,
   https://doi.org/10.1016/j.procs.2021.01.079
10. Application of attitude tracking algorithm for face recognition based on OpenCV in the intelligent door lock
    Publisher: ScienceDirect,
    https://doi.org/10.1016/j.comcom.2020.02.003
11. Current state of API security and machine learning Using Sensors and RFID,
    Publisher: IEEE,
    https://ieeexplore.ieee.org/abstract/document/9778101
12. Survey of machine learning techniques for malware analysis
    Publisher: ScienceDirect,
    https://doi.org/10.1016/j.cose.2018.11.001