International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

End to End Encrypted Smart Lock Using RSA based on Opinion from Social Media Review Comments

Dr. S. Revathi[1], Dr. Shreedevi[*2], Dr. K. M. Monica[3], Dr. Bindu G[4], Mrs. D. Menaga[5]
[1]Professor, Department of Computer Science and Engineering
B.S.Abdur Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.
Email: srevathi@crescent.education
[2]Asst. Prof (Sl.Gr.), Department of Computer Applications
B.S.Abdur Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.
Email :shreedevi@crescent.education***Corresponding autho**r
[3]Assistant Professor,
Senior Grade 1, SCOPE, VIT, Chennai.
Email: Monica.km@vit.ac.in
[4]Associate Professor,
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.
Email:bindugarikapati7@kluniversity.in
[5]Assistant Professor, CSE Department,
St.Joseph's Institute of Technology, Chennai
Email:dev.menaga@gmail.com

Abstract— In the modern era, from big apartments to small houses, startups to corporate buildings, protecting assets or preventing unauthorized persons are crucial problems. Often traditional locks like padlocks are prone to security risks since they can be easily bypassed. Existing smart lock systems are prone to Man in middle Attacks where digital keys can easily be duplicated. The review comments about prevailing smart locks technologies have been collected from various sources such as blogs and microblogs. The data set is analyzed to discover the opinion of the people about the smartlock product. In this proposed system, an innovative smartlock system prototype is designed using current technologies. A smart lock system has been proposed which is encrypted end-to-end using the RSA algorithm. This system uses a one-time password sent to registered users combined with the master code to unlock the door. This system is designed as such only the users who are connected to a wireless local area network are able to access the smart lock system, this adds an additional layer of security. It is connected to the cloud and logs all the activity from booting to shutting down. The breach detection system along with image capture is also included to detect forced intrusions. The client functionality can be easily ported to any platform which supports HTTP protocol which tends to be the major advantage of the proposed work.

Keywords- Smart Lock, RSA, Door Lock System, HTTP Protocol, Opinion Mining.

I. INTRODUCTION

Digital home security and automation are becoming more unavoidable nowadays. Since smart locks only provide access to authorized users, smart locks are more secure and reliable when compared with the existing traditional lock system, since traditional locks can be bypassed easily with physical tools. Intruders are less likely to attempt a break-in if a home security system is already installed, according to data. The traditional lock system remains the same all these centuries and the other technologies are drastically changing day by day. The key-lock system was invented 4000 years ago and people use the same lock system till now. These kinds of locks are embedded in the door mechanically thus it requires manual effort to unlock the door. In recent times, the Internet was enhanced and all electronic devices were connected to it. In order to make the devices faster and smarter, electronic appliances are connected to the Internet. The number of mobile users increases every day. Useful smart applications have also been established. Nowadays smartphones are used for a variety of purposes such as answering calls or sending messages, smartphones are also used to control various appliances through the Internet with the help of a mobile application. People use the traditional key-lock system which has a few drawbacks such as misplacing keys etc. The analysis of smart lock reviews reveals the fact that most people are not satisfied with the existing smart lock systems and it has been conveyed through negative opinions.

To eliminate these kinds of drawbacks, smart locks are developed where the user can unlock the system through the smartphone with the help of a smart application.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

II. MOTIVATION BEHIND THE WORK

Digital home security and automation are becoming more unavoidable nowadays. Since smart locks only provide access to authorized users, smart locks are more secure and reliable when compared with the existing traditional lock system, since traditional locks can be bypassed easily with physical tools. The statistics show that intruders are less likely to attempt to break into a home where there is a home security system already enabled. The traditional lock system remains the same all these centuries and the other technologies are drastically changing day by day. Most of the existing systems involve the existence of Man-in-the-Middle Attacks which means any individual can easily make an attempt to unlock the system using certain existing algorithms. Some existing systems consist of a Central Control Module within the door itself which is required to reduce additional complications to the door. Most of the existing systems are designed in such a way that the WIFI or the Bluetooth which serves as the Central Control Module to the smart lock tends to be open which is too easy for individuals to brute force them and unlock the door in case. Our proposed system has been built in such a way that it tends to reduce the major disadvantage in the existing systems. Our proposed system provides two levels of security to the users in order to minimise Main-in-the-Middle Attacks.

- End-to-End Encryption
- Two Factor Authentication

The details entered by the user in the client device are encrypted using the RSA algorithm to enforce end-to-end communication. A unique ID for every user is generated along with the authentication token for the client device. All the details of the user are stored in the cloud for easier accessibility and maintainability.

Two-factor Authentication is categorized into two divisions

- Something we have
- Something we know

Something we have refers to OTP generated which is made available for the users on their mobile phones and something we know is the master key. The user must enter both the OTP and the Master key in order to access these cured areas or to unlock the system.

III. CONTRIBUTION OF THE PAPER

Here, in this work, Raspberry Pi, camera, and buzzers are used for security purposes. To secure the communication between the smart lock and the smartphone, the RSA algorithm is implemented. The details of the client are encrypted using the public key which is accessed by the client devices and the details are decrypted using the private key that is stored in the system itself. For the purpose of security, RSA keys are newly generated every time the lock system boots up. The smart lock system can only be accessed within the wireless local area network. It's up to the owner's decision to set up a WPA2 password for the WIFI or not. If the WIFI is secured with WPA2, then this WIFI acts as an extra layer of security where it allows only the users to connect who know the WIFI password.

To unlock the door, the user has to be registered first using their mobile number. The registered users will receive a token that is stored in the smartphone. This token is used for authentication. To unlock the door, the user or owner has to request the smart lock system using the client device which in turn system sends a one Time Password to the mobile number which is already registered. After receiving the One Time Password, the user has to enter the received One-Time Password along with the master key. Not knowing either of them will not unlock the door. Signature checks for tokens are implemented in the smart lock to ensure the token data integrity or to check if it was tempered by any malicious user.

Redis database is used as a message broker between the smart lock API and enter tehr the hardware controller and also to store data like Master key hash, OTP and RSA keys for validation. Breach detection is also implemented to check if the door is breached, if the door is breached then the buzzer/speaker turns on and the alert SMS is sent to the administrator.The owner's data is manually configured when the system is setup for the first time. LCD 16x2 display can be included to show the IPaddress, statusand errors of the system. Moreover, to increase the accessibility, a static IP address can be assigned to the smartlock.

IV. RELATED WORK

Abdallah Kassem et al(2016) proposed a prototype of a locking system designed using recent technologies. The usage of Digital Information such as secret codes will result in a more secure path in any kind of locking system. Technically, this system has also been embedded in the Local Area Network of the house. This locking system is secured since it has prevented the users to access the system only through the network. The door can be opened using the Smart Lock Client System which leads to a wide range of innovations, particularly in locking systems. This prototype lacks security concerns since it is prone to Man In The Middle Attack, where a malicious user can intercept the insecure communication channel and record the digital keys recursively and send it again through the insecure communication channel to unlock the system.

PradipTilala et al(2017) presented a smart locking and unlocking system for residential door security. According to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

their suggested solution, the door lock is operated by an Android App that talks with a WeMos D1 WI-FI module that is already incorporated into the door lock via WI-FI. To send messages, the Firebase cloud messaging service was also used and has been implemented to send OTP to the client's android phone. This system has eliminated the need for an embedded GSM module. A unique password has been associated with the client application for secure access to the door lock system. Their system is set up in such a way that it checks the user's credentials before sending an OTP to the mobile app interface via the Firebase cloud service. The limitation of this prototype is that the OTP is sent to the application instead of a user's cellular number, anyone having the application or access to cloud service can open the door.

Yong Tae Park et al. (2009) suggested a unique ZigBee-based home automation system that combines home security and automation. The main advantage of their proposed system was that their system can be easily fixed without the need for any infrastructure and proper planning. Their proposed solution also makes full use of ZigBee's capabilities for monitoring and regulating the home's surroundings and condition via the digital door lock. Because their suggested system is based on a wireless sensor network, it is a low-cost, adaptable, and simple-to-install system that does not require any prior design. However, the disadvantage is, if the system is breached by a malicious user or hacker, the whole house will be compromised since the hacker can gain access to all the sensing and controlling modules.

Trio Adorno et al(2019) proposed a prototype for IoT and GPS-enabled door lock systems. The main objective of this research was to design a door lock system that does not depend upon any manual input from the user but also remains secure. The advantage of this system is simplicity, where no inputs or interface is needed for the user to unlock the door. However, the disadvantage is the location or GPS coordinates can be spoofed easily by a malicious user or a hacker to unlock the door.

Naser Abbas Hussein et al (2017) proposed a security door lock system that is entirely based on Raspberry Pi technology and includes cameras, a keypad, and pi-lids that are used to provide an alarming system that can both notify the owner and recognize visitors by providing them with a user-id. Only authorized individuals will have the ability to access the door. This system allows a user if they know the password, if not, their face is captured using a pi camera and a face recognition algorithm has been applied to check if the guest/user's face is already registered and allowed access to unlock the door. The advantage of this system is the low-cost setup and simplicity. However, the system can be easily breached by showing a photo of a registered user to the camera. Also, face recognition systems using cameras do not work in low-light environments.

NareshkumarR.Metal(2017) developed a door automation application using Raspberry Pi and GSM modules. In this paper, Biometrics has also been used as an additional security purpose which increases the security level. The system sends the image to the owner asking if the guest is allowed or not. Based on the owner's choice the door lock is handled. If the system crashes or is unable to send the images to the owner, a Biometric scanner is used as a backup authentication system. The authors have designed the system in such a way that it has minimized human efforts and has provided security throughout the system. The major advantage is that needed actions can be executed in a relatively brief period of time. However, the disadvantage is that the owner should have the application connected to the internet all the time to receive images, or an intruder can just send fake images to the owner to unlock the door.

Nayana R. and Shashidhar R(2019) have proposed a system that has made use of a fingerprint sensor, a GSM module, and an Arduino microcontroller. With the help of a matching algorithm, the fingerprints of the authorized individuals have been stored and it has been checked whether the person is authorized or not based on the algorithm. An OTP has been generated and it has also been sent to the person's mobile phone with the help of a GSM Module. This action takes place only if the person is authorized. If the fingerprint does not match, then it denotes that the person is unauthorized and OTP will not be sent to the person's mobile phone instead an indication will turn on denoting that some unauthorized individual has tried to access the door. Their proposed system has been implemented in areas where security plays an important role such as banks, offices etc. The limitation of this prototype is that many fingerprint sensors can be overridden by hardware tweaking. And also, the internet needs to be available all the time.

Uzma Fatima Shaikh et al(2019) has proposed a smart door lock security system with the help of face recognition technology and One Time Password (OTP) which has been generated using GSM. With the help of the proposed system, the usage of keys can be easily reduced to a greater extent. Thus, this paper has provided a cognitive structure in order to provide the purpose of security with easy service and cost efficiency. Since facial recognition and OTP generation plays a major role the proposed system is highly effective for secured areas. The advantage of this proposed system is the simplicity of the working mechanism. However, PCA is a classic algorithm that is replaced with many new face recognition algorithms because of efficiency, also face

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

recognition does not work in low light environments since images are captured using the camera.

Muhammad Ahtsham et al(2019) have proposed a locking system built using cryptographic algorithms. They have proposed the system in such a way that the system has been based on passwords and is cryptographically encrypted. In this paper, a highly secured door lock system has been presented. In order to interact with the CryptoLock a smart Application has been developed. Various Cryptographic algorithms have been used in CryptoLock in order to guard the data transmitting over the network. Thus, the proposed system has provided easy access controls unauthorized access, and also protects user data. Cameras can be added in the future to increase the level of security by one step. However, the malicious user can sniff the encrypted data packets and he can send it again through the channel to unlock the door.

Md.Maksudur Rahman et al(2018) have proposed a system to implement a password-protected electronic lock system which has provided great security and has reduced the usage of traditional locks. The ultimate goal of this system was to develop a locking system that provides high security as well as cost efficiency. The proposed system has been easy to implement. In the proposed system, the keypad acts as the input, the LCD display as the output module and the Microcontroller chip has been used as the controlling unit. The lock system has been safeguarded by a password that has been set by the user. Only authorized persons can change the password which tends to be more secure when compared with the other systems. While changing the password, a secret code that is known only to authorized individuals must also be entered in order to change the password. Thus, the security system has also been implemented in all stages of the system. The present security system which is available in the outside world is expensive to implement and use. Thus, they have designed a prototype that has been cost-efficient and easy to access. Their prototype has been more reliable and user-friendly. However, the malicious user sniffing the data packets in the insecure communication channel can extract the secret code and thus can compromise the whole system.

Anshika Agarwal et al(2017) proposed a system that has allowed the user to control his door lock with the help of Bluetooth or a message over the internet. The user has to keep a track of who visited his/her home in order to preserve the security functions in the proposed system. The proposed system has been designed in such a way that it has limited the cons of the existing system and has also provided high-level security to the users. The proposed system has been cost-efficient since it works on the basis of motion sensors. The person is categorized as an intruder or visitor based on the ringing of the bell. The system has been proven to be much more useful and it has also been more efficient when compared with the other ineffective existing systems. This system's major goal is to ensure the security of the home and to provide a smart way to lock and unlock the door. Thus, the results have shown that the proposed system has served as a complete solution for security issues.

Siddhi Kavde et al. (2017) developed a system for developing an application for those who work outside the home and want to grant remote access to a servant or any other authorized individual to enter the house. This system helped physically challenged people to operate the door lock without hassle. The major advantage of this system is it helps the administrator or owner to have control over their workplace/home from anywhere at any time. The drawbacks of this system are using the insecure communication channel via Bluetooth which is prone to MITM attacks and NFC tags can be easily duplicated.

AkhilSriram et.al (2021) collected the dataset about IoT devices from Twitter and Reddit users. Sentiment analysis is carried out over the data set by using the BERT algorithm. The outcome of the analysis shows the negative opinions and positive opinions of Reddit and Twitter users respectively about privacy and IoT devices security reviews. The user's opinion varying time to time which is done with a longitudinal study.

V. SYSTEM ARCHITECTURE

The architecture of the proposed system is shown in Fig.1. Except LCD Display, the other modules are embedded in the proposed system which enables two-way communication with the raspberry pi. Raspberry Pi is a low-cost board that is available and it is a miniature of the computer which can perform some basic operations as the computer does. Cloud storage supports two-way communication as it stores the log details and it is also useful to insert and retrieve data from the cloud. The client devices connect to the system with the help of HTTP protocols using a wireless network technology such as WIFI. Redis is a caching database. The main advantage of using a caching database is that it is faster compared to the other existing databases. Redis offers data replication and can also withstand failures to provide uninterrupted service. Redis is easy to implement in Raspberry Pi. The camera helps to take snapshots of an individual whenever an incorrect password is entered. Thus, the camera is helpful for the owner to detect the intruder who has tried to access the smart lock. The LCD display is enabled for the user to know the current status of the lock whether it is locked or unlocked. A lock is connected with the Raspberry Pi in order to make respective arrangements (i.e.) when a user locks or unlocks the door, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

lock receives a signal from the Raspberry Pi to perform the command that the user expects.

Breach Detection or Alert Speaker is also enabled in the proposed system to ensure whether it is the user or some unauthorized individual accessing the smart lock. Suppose if an individual enters an incorrect password or tries to break down the door in order to access the secured area then the closed circuit opens up, the alert buzzer is turned on and alert SMS is sent to the owner.

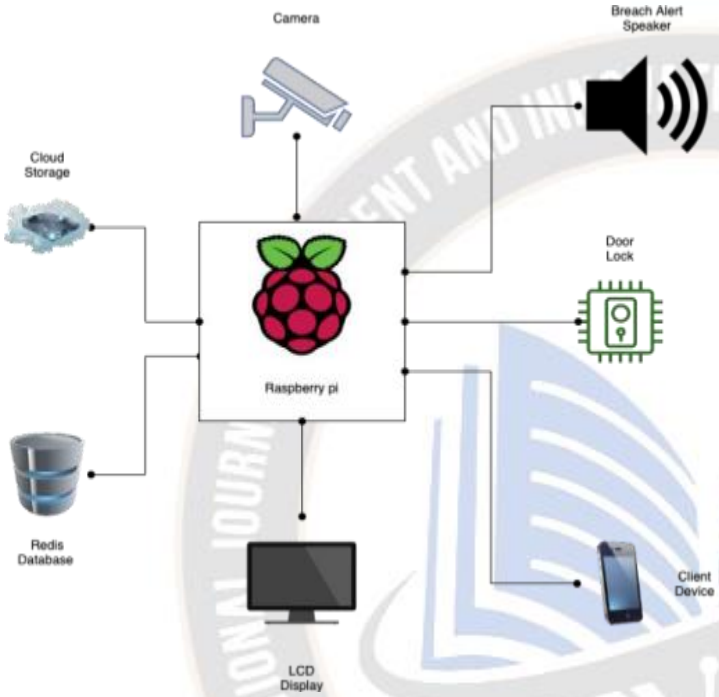

Fig. 1 System Architecture Diagram

VI. IMPLEMENTATION

A. System Initialisation

The overall system architecture describes the system flow which is managed when the corresponding operations are carried out. Fig. 2 denotes the flow of system initialization. The first stage which means the initial stage a program or an operation is started. The system checks whether the Internet is connected. If not connected, it waits until the successful connection is established. On the other hand, if the internet is connected the system starts to generate a 3072-bit RSA public key and the private key. Internet must be needed in order to send OTP and for the cloud functions to work properly. Redis Database stores both the public key and private key of RSA. The main program sends/saves the controller status as 'RUNNING' in the Redis database as soon as the keys are stored in the database. This status is captured by the controller script and starts the lock/unlock operation. In case there is any system error or the user intentionally decides to abort the operation then the shutdown operation is carried out where the system stops its process of further being executed.

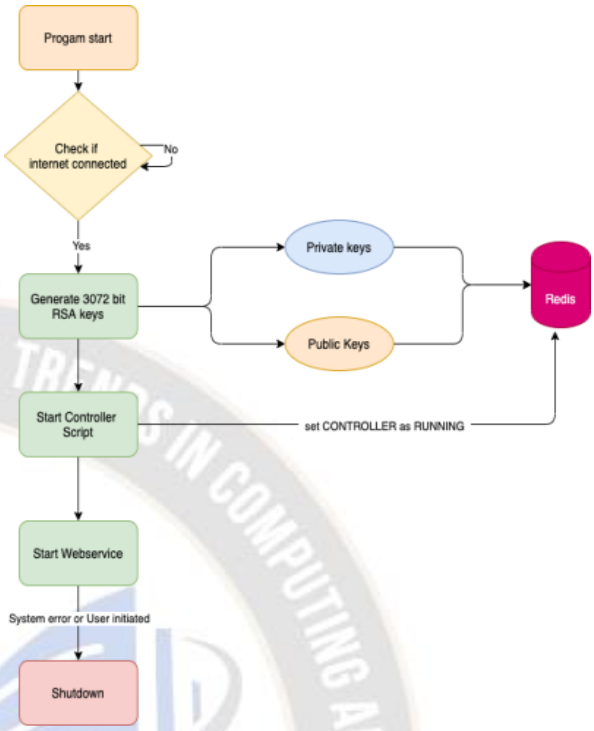

Fig. 2 System Initialisation

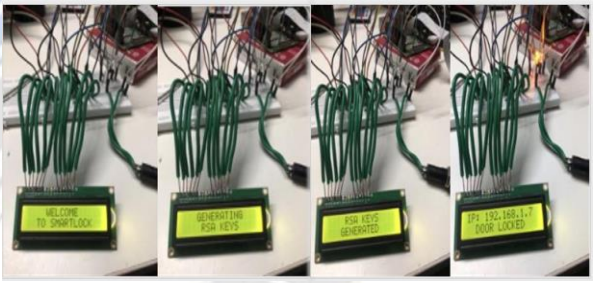

Fig. 3 Hardware Setup for System Initialization

B. Controller Initialization

The first stage includes the controller script which is responsible for the raspberry pi board operation. The Raspberry Pi setup is divided into two categories:

1. PCM
2. Board

Fig. 4 clearly denotes the flow of controller initialization. Here, in this system, Raspberry Pi has been set up using the board category. The controller script status is received from the Redis database. After the controller script begins to start its operation, the system receives the door status. The system checks whether the door status is changed. If yes, the system checks whether the door is locked or unlocked. If the output remains to be yes then the door is locked otherwise the door is unlocked.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

If the door status remains unchanged then, the system checks whether the push button is pressed. The system unlocks the door if the push button is pressed. The system checks if the door is breached by any of the intruders if the push-button is not pressed.

If the door is breached, a sound alert is raised by the alert speaker. If the door is not breached, the system checks whether the controller status is running or in an idle state. The same process is repeated in a loop until the door is locked/unlocked.

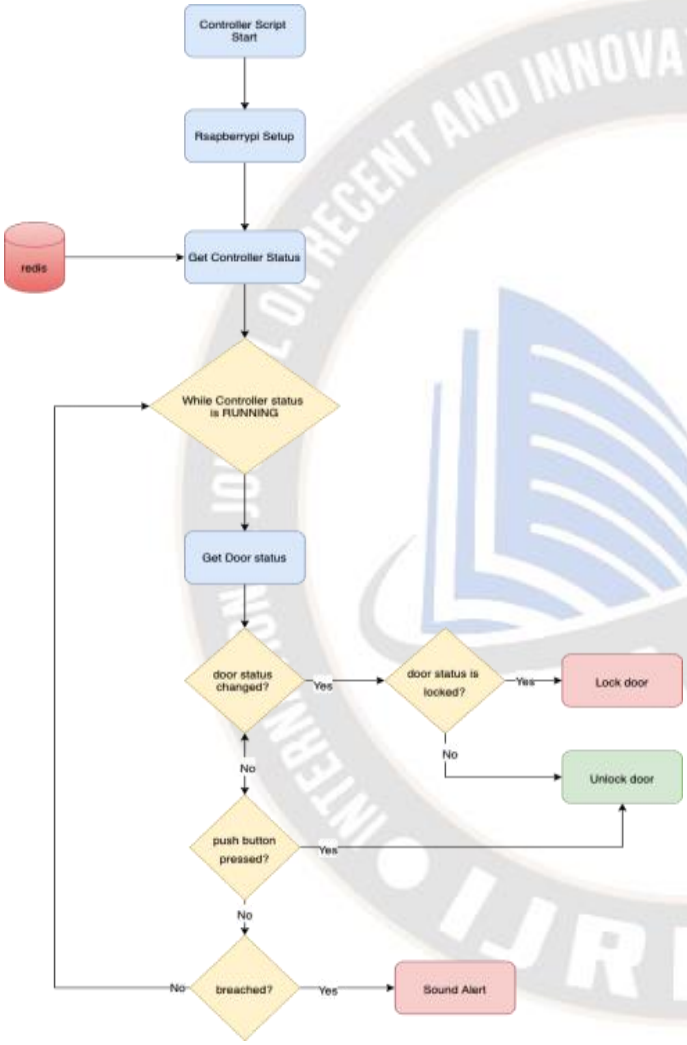

Fig. 4 Controller Initialization

Fig. 5 Hardware Set up for Controller Initialization

C. User Registration

Here, Redis Database stores a master key which is hashed using the SHA-256 hashing algorithm, and also stores a private key. SHA-256 itself is not a cryptography algorithm but it enables us to store alternate forms of data which can be used to compare with other hashed data. Hashing algorithms are prone to brute-force attacks. An attacker can hash various guessed plaintext data and compare it to the stored hash to find the data. SHA256 is used to slow down the brute force technique. The master key, name, and mobile number of the client are encrypted using the public key by the client. The deciphers received are decrypted using a private key which is already stored in the Redis Database. The hashed master key received from the client is cross-checked with the original master key hash stored in the Redis database. If both the master keys matches, the name and mobile number of the user is stored in Cloud, and UUID(UniqueUserID) is generated. This UUID can be used to fetch the user's details from the cloud and can be used to log when that user locks and unlocks the door. This UUID is used to generate a unique token which is then sent to the client app. The client app will authenticate itself using this token. This token is designed in such a way if any of the data has been tampered with, the signature verification will fail and the token is invalidated. The front-end design is given in Fig. 6.

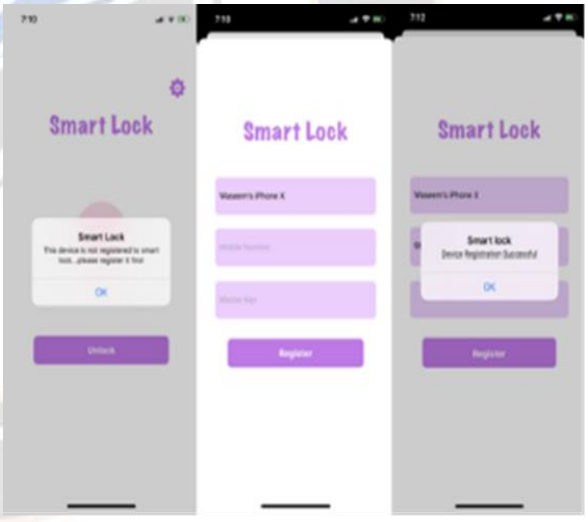

Fig. 6 Front End Design for Registration

The token is generated using UUID and the master key. If some malicious user tries to change the UUID which is stored in base64 format without knowing the master key, then the token gets invalidated. This token can be used by various modules for authentication and authorization. Fig.7 denotes the working of the registration module.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
Article Received: *26 June 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *04 September 2023*

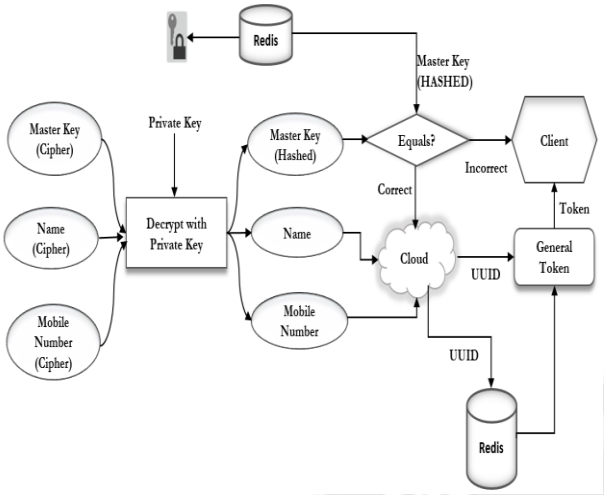

Fig. 7 Flow Diagram and Front Design for Registration

D. OTP Generation

- The token which is received by the Client app is decrypted here and a signature check is performed to check the token data integrity. If the signature check validates, UUID stored in the token is retrieved and the user's mobile number is fetched from the cloud database. Once the registered mobile number is fetched, a 6-digit OTP is generated and the OTP plaintext is sent to the registered mobile number.

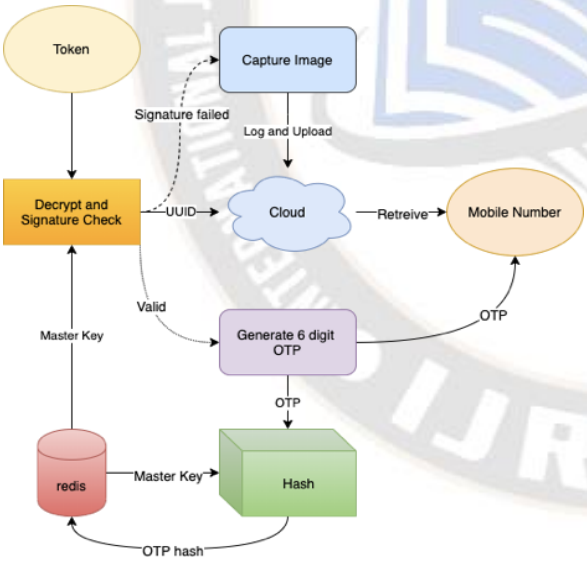

Fig. 8 OTP Generation

At the same time, the OTP generated is appended with the master key hash stored in the database is hashed again, and stored in the Redis database with the key "ACCESS_KEY_<UUID>".

The OTP is hashed as Eq. (1)

SHA256(OTP + SHA256 (master key)) ---- (1)

The OTP is added with the hashed master key and in turn, the OTP is hashed again to ensure the brute force attack against OTP fails. This technique also ensures system security if the registered device is compromised to receive the OTP SMS without knowing the master key. One should know both the master key and OTP to unlock the smart lock. If the token is invalid or a signature check failed, the Image is captured and this incident is reported or logged in the cloud database. Fig. 8 denotes the flow of OTP Generation and the front-end design is given in Fig. 9.

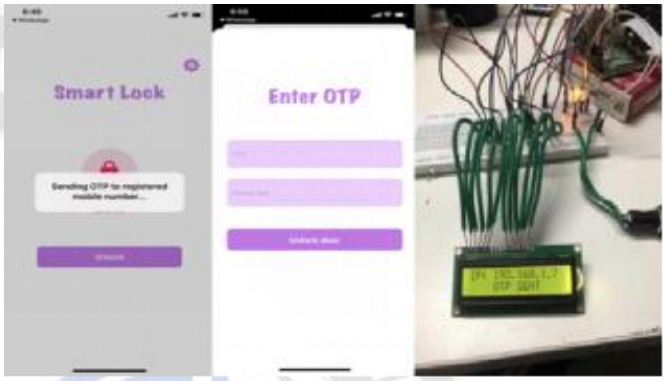

Fig. 9 The Front-end Design for OTP Generation

E. OTP Validation And Door Unlock

The token received from the client is decrypted and the maintenance of the data integrity of the token is verified with the help of a signature check. If the token is valid, then the encrypted OTP which is received from the client is decrypted using a private key stored internally in the Redis database. Once decryption completes, the hashed OTP received is cross-checked with the OTP hash stored in the Redis database. If the OTP hash matches, the door is unlocked and logged to the cloud.

If the token is invalid or a signature check failed, the Image is captured and this incident is reported or logged in the cloud database. Fig. 10 denotes the flow diagram for the validation of OTP and front-end design is given in Fig. 11.

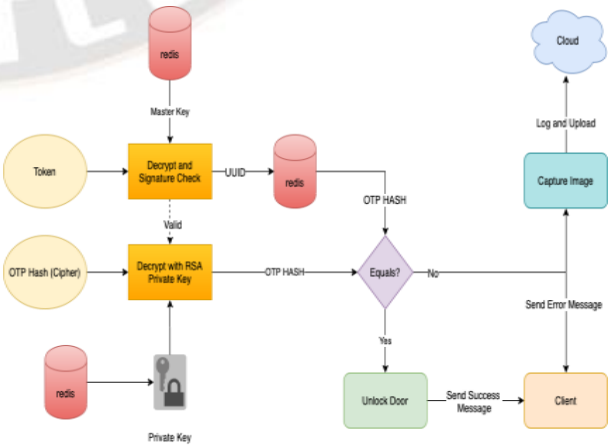

Fig. 10 Flow diagram of the OTP validation

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

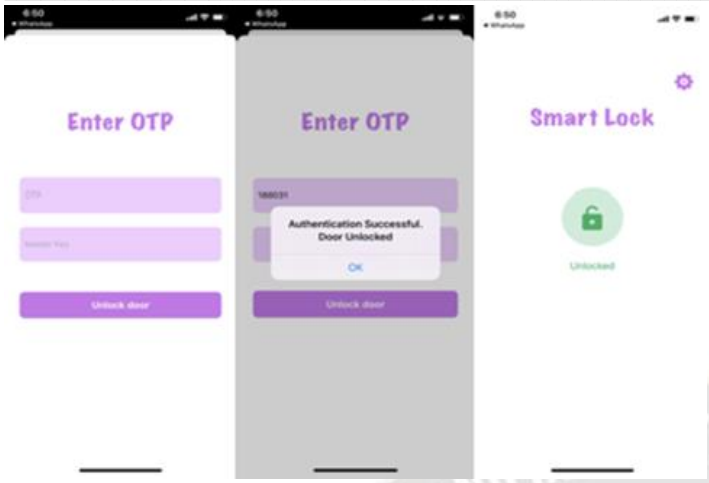

Fig. 11 Flow Diagram for the Master Key Modification

F. Master key modification

This module can only be accessed inside the system, to change the master key the owner should log in to the system and run the change master key program or just call the change master key HTTP endpoint. This module works by getting the master key currently in use and the new master key. The master key currently in use is hashed using the SHA256 algorithm and cross-checked with the master key hash that is stored in the Redis database. If the master key currently in use matches with the master key stored, then the new master key is hashed using SHA256 and stored as the master key in the Redis database.

However, if the master key is changed, all the tokens generated are invalidated since the master key is changed and the token signature check will fail. So, all the users have to register their client app again to receive their new tokens. Fig. 12 picturizes the change of the master key with the help of a flowchart.

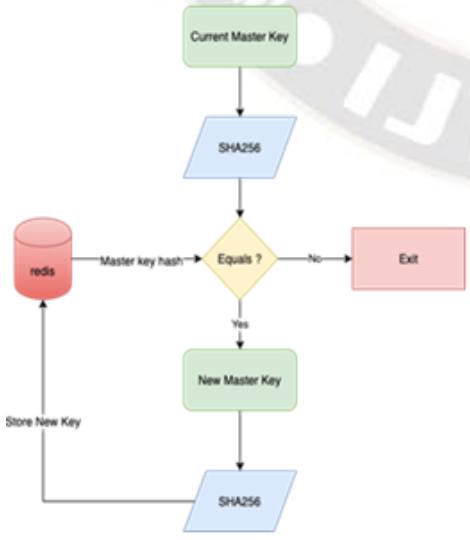

Fig. 12 Flow diagram for the master key modification

VII. CONCLUSION AND FUTURE SCOPE

Opinion Mining helps us to make decisions on purchasing products. In this work, we have analyzed the comments posted by the users about smart lock systems and the negative opinions taken into consideration for implementing the work for a more secure and efficient smart lock system. Thus, an end-to-end encrypted smart locking system using RSA with breach detection is proposed. The proposed system is low cost and can be easily installed in various environments from home to office, banks to server rooms. The API nature of the proposed system allows flexibility since the client app can be ported or made for every platform that exists which supports HTTP protocol. The structure of API can easily be understood by the administrator or developer which will help add more modules to the system. The use of RSA makes hackers difficult to break the encryption securing the communication channel to send/receive messages between the system and the client. The modules which were made use of in the system are easily available and cost-efficient. This system can completely replace the traditional lock system and reduce the hassle of maintaining different keys for different locks. Hence increasing the security and usability of the locking system.

RSA keys size can be reduced to improve the speed of the overall system. Authentication systems like Fingerprint or Face recognition can be implemented as a Backup Auth system in case of system or network failure. Client App can be ported to Windows, Mac OS, Linux, Progressive Web apps, etc.

REFERENCES

[1] Shi C, Roy D, Krivenko P (2006) Alkali-activated cements and concretes. CRC Press, Boca Raton
[2] Davidovits J (1991) Geopolymers. J Therm Anal Calorim 37:1633–1656
[3] Okamura H., Ouchi M. Self-compacting concrete. J. Adv. Concr. Technol. 2003;1:5–15. doi: 10.3151/jact.1.5.
[4] A. U. Zaman, A comprehensive study of the environmental and economic benefits of resource recovery from global waste management systems, J. Clean. Prod. 124 (2016) 41– 50. https://doi.org/10.1016/j.jclepro.2016.02.086.
[5] A.M.N. Kashyap “Prediction Of Setting And Strength Characterstic Of Binary Blended Geopolymer Matrix”, i-manager’s Journal on Structural Engineering, Vol. 6 l No. 4 l December 2017 - February 2018
[6] Mallinadh, A.K., Chandra Sekhar Rao, T., Ramana Rao, N.V. (2020). Strength and Behavior of Hybrid Fiber-Reinforced Geopolymer Concrete Columns Under Uniaxial Compression. In: Pancharathi, R., Sangoju, B., Chaudhary, S. (eds) Advances in Sustainable Construction Materials. Lecture Notes in Civil

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8100
***Article Received:** 26 June 2023 **Revised:** 25 August 2023 **Accepted:** 04 September 2023*

Engineering, vol 68. Springer, Singapore. https://doi.org/10.1007/978-981-15-3361-7_1

[7] M. Maroof, N. ., & Abdul Waheed, M. . (2023). Energy Efficient Clustering and Routing using Energy Centric MJSO and MACO for Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 213–221. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2648

[8] Kashyap A.M., Rao T.C.S., Rao N.V.R. (2021) Durability Performance of Binary Blended Geopolymer Concrete. In: Abdel Wahab M. (eds) Proceedings of 1st International Conference on Structural Damage Modelling and Assessment. Lecture Notes in Civil Engineering, vol 110. Springer, Singapore. https://doi.org/10.1007/978-981-15-9121-1_15

[9] N. Palankar, A. U. R. Shankar, B. M. Mithun, Investigations on Alkali-Activated Slag / Fly Ash Concrete with steel slag coarse aggregate for pavement structures, Int. J. Pavement Eng. 8436 (10) (2015) 1–13. https://doi.org/10.1080/10298436.2015.1095902.

[10] Mr. Dharmesh Dhabliya, Prof. Ojaswini Ghodkande. (2016). Prevention of Emulation Attack in Cognitive Radio Networks Using Integrated Authentication . International Journal of New Practices in Management and Engineering, 5(04), 06 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/48.

[11] B. M. Mithun, M. C. Narasimhan, N. Palankar, and A. U. Ravishankar, Flexural Fatigue performance of Alkali Activated Slag Concrete mixes incorporating Copper Slag as Fine Aggregate, SSP-Journal Civ. Eng. 10 (1) (2015) 7–18. https://doi.org/10.1515/sspjce-2015-0001.

[12] Kushal Ghosh and Dr.Partha Ghosh, "Effect of %Na 2 O and %SiO 2on apparent porosity and sorptivity of fly ash-based geopolymer," IOSRJournal of Engineering, Vol.2, no.8, Pp: 96–101, 2012.

[13] Wardhono, A. (2019). Comparison study of class F and class C fly ashes as cement replacement material on strength development of non-cement mortar. IOP ConfSer Mater SciEng, 288.

[14] Alexei Ivanov, Machine Learning for Traffic Prediction and Optimization in Smart Cities , Machine Learning Applications Conference Proceedings, Vol 3 2023.

[15] Mallikarjuna Rao, G., &Gunneswara Rao, T. D. (2015). Final setting time and compressive strength of fly ash and GGBS-based geopolymer paste and mortar. Arab J SciEng, 40(11), 3067–3074.

[16] Al-Shether, B., Al-Attar, T. S., Hassan, Z. A., AlShathr, B. S., Al-Attar, T. S., Al-Shether, B., AlAttar, T. S., & Hassan, Z. A. (2016b). Effect of curing system on metakaolin-based geopolymer concrete. J Univ Babylon - EngSci, 24(3), 569–576.

[17] Alanazi, H., Yang M., Zhang, D., & Gao, Z. (2016). Bond strength of PCC pavement repairs using metakaolin-based geopolymer mortar. Cement Concr Compos, 65, 75–82. https://doi.org/10.1016/j.cemconcomp.2015.10.009- DOI

[18] Alanazi, H., Yang, M., Zhang, D., & Gao, Z. (2017). Early strength and durability of metakaolinbasedgeopolymer concrete. Mag ConcrRes,https://doi.org/10.1680/jmacr.16.00118

[19] Nath, P., &Sarker, P. K. (2017). Flexural strength and elastic modulus of ambient-cured blended lowcalcium fly ash geopolymer concrete. Construction and Building Materials, 130, 22–31.

[20] Ma, S., Zhang, Z., & Liu, X. (2022). Comprehensive Understanding of Aluminosilicate

[21] Joseph Miller, Peter Thomas, Maria Hernandez, Juan González, Carlos Rodríguez. Machine Learning for Decision Support in Uncertain Environments. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/205

[22] Phosphate Geopolymers: A Critical Review.Materials (Basel), 15(17), 5961. doi: 10.3390/ma15175961.

[23] Muthadhi, A., Vanjinathan, J., &Durai, D. (2016). Experimental investigations on geopolymer concrete based on Class C Fly Ash. Indian J SciTechnol, 9(5), 1–5

[24] Hardjito, D., Wallah, S. E., Sumajouw, D. M. J., &Rangan, B. V. (2004). On the development and properties of low calcium fly ash geopolymer concrete. ACI Mater J, 101(6), 467–472.

[25] Karthik A, Sudalaimani K, Vijaya Kumar CT (2017) Investigation on mechanical properties of fy ash-ground granulated blast furnace slag based self-curing bio-geopolymer concrete. Constr Build Mater 149:338–349.