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, April 2025
Impact Factor: 7.67

Smart Lock Device

Abhay Gawade, Atharva Bhor, Prof. Shradha Linge
MIT-ACSC, Pune, Maharashtra, India
Assistant Professor, School of Computer Science, MIT-ACSC, Pune, Maharashtra, India

Abstract*: This Project includes smart lock enhanced with biometric which includes fingerprint as well as voice recognition system. This Device will have its own dedicated app and website. For implementing this project, we will be using a fingerprint sensor, microcontroller, microphone, Gsm Module, Motors and necessary hardware components. Smart Lock will not be only restricted to main door locking system but also have other models which will be suitable to lock doors, cabinets, wardrobe(sliding, openable) and also aldrop!. The lock will be designed according to known hardware synopsis. The purpose of introducing this smart lock is to give more security to the user which will not bound only to specific doors. Smart Lock Device will have integrated fingerprint sensor with mic. The purpose of introducing microphone with fingerprint sensor is to ensure more security to the user. Fingerprint Sensor will be associated with number of invalid fingerprint attempts. The software system of this lock device will be designed in such a way that user has to sign-up initially with their contact number as well as email id. Once the user has logged-in successfully they'll have to pair their Smart Lock Device with their phone. If Someone has exhausted number of Invalid fingerprint trials. The user will immediately receive notification that someone is trying to Breach The lock System with an option if they want to enhance security, if user allows that option, the lock will immediately turn on voice recognition and will unlock only when user Speaks as well as Place Finger on the sensor. The Purpose of Collecting Contact Number & mail id is when user is offline, user will receive a text message on their given phone number as well as on given mail id. In Software update, we can introduce the feature of adding contact info of neighbors as well, so that neighbors can also receive pop-up notification, if user wishes to inform them. Keywords- Biometric, Lock, Breach, Security, Voice..*

Keywords: smart lock

I. INTRODUCTION

Traditional vs Smart Lock What are traditional locks?

The term 'traditional locks' is not something that many people are used to hearing. Granted, there are many different types of regular locks that are not automated, but up until smart locks carved out space for themselves, these old locks

DOI: 10.48175/568

were just called locks. There are many variations of traditional locks, which can be used for a plethora of purposes. The term is essentially referring to locks that are not automated and locks that have to be manually engaged in order for the locking mechanism to be operated.

How do traditional locks work?

The majority of traditional locks work when a key is used to activate the locking mechanism, which will give it the ability to lock or unlock. Some very common examples of these traditional locks are pin tumbler locks, rim locks, and mortise locks. Let’s take a look at the pin-tumbler lock for example.

Pin-Tumbler locks are some of the most common locks used within residential properties. The locking mechanism in these locks features a series of spring-loaded pins that are in turn loaded into cylinders. The cylinders consist of a set of pins that are designated as the key pins and the driver pins. When the correct key is inserted into the locking mechanism the key pins are elevated, which pushes the driver pins upward.

Once the proper key is inserted into the lock, the driver pins and key pins align at the shear line. Then the key can be turned in the lock, to unlock, and sometimes lock, the mechanism. If the wrong key is used, the misalignment of the pins will block the key from being turned because the pins will be bound at the shear line.

How secure are traditional locks?

This is not an easy question to answer, and that is due to the number of lock variations that homeowners utilize. The security levels that these locks give homeowners varies. For instance, the deadbolt is one of the most common exterior residential locks. There are usually two main types of deadbolts, single cylinder deadbolts, and double cylinder deadbolts. These locks are known to provide maximum security for homeowners but only if the right ones are used and if they are used in the right way.

Deadbolts are grouped according to grades that determine their relative strength. These grades are usually based on the relative strength, longevity, and durability of these locks. They range from 3 to 1, with 3 being the lowest grade and 1 being the highest grade. ANSI (American National Standards Institute) Grade 1 deadbolts provide homeowners with the maximum security for their residential locks. However, the thing that allows these locks to be as secure as they are, are the additions that can be made to ensure that they are as secure as possible.

What are smart locks?

In their simplest form, smart locks are automated versions of traditional locks. In most cases, a smart lock will make use of the traditional lock mechanism, but the lock mechanism can be engaged electronically or remotely. These locks are different because they require a different interaction (between the user and the lock) than traditional locks. The name ‘smart locks’ also stems from their ability to be controlled and operated by smart phones, as well as their ability to integrate with other smart devices.

These locks allow homeowners to control and monitor their locks in a way that traditional locks do not. If the smart locks are working the way it is intended to, it provides unparalleled ease of access and comfort. However, this does not always mean it is the most secure option. Smart lock manufacturers tend to focus more on the efficiency and added features that the lock brings to the table, which makes them skimp on the security factors that have made locks a hallmark for every home.

How do smart locks work?

Smart locks, much like traditional locks, require a lock and a key in order to work properly. A smart lock has to receive its operational instructions from a pre-authorized device, as well as a cryptographic key in order for it to perform its locking and unlocking process. In addition to this, smart locks are also able to monitor the status of the lock and send pertinent alerts to authorized devices. In most cases, this would be the homeowner’s smart phone. These locks are considered to be a huge part of the smart home, and they are capable of integration with many other smart devices and products

The key for smart locks is not a physical key as it is for traditional locks. These keys are either special key fobs or a set of instructions issued by home automation protocol, which will authenticate that it is the proper key for the lock. Some smart locks also have the ability to hand out temporary keys to third parties, and these temporary keys function as spare keys.

How secure are smart locks?

The security of smart locks has been in question since before their inception. It did not become apparent to many people that this was even an issue until after homeowner’s started to acquire smart locks. This might have been because smart locks were not necessarily advertised for their security capabilities, but they were marketed by talking about all the new and cool things that a smart lock could do for an individual’s home. For instance, some smart locks give homeowners the ability to remotely monitor the status of their locks, as well as remotely operate their locks. These features are some of the things that make a smart lock truly unique and the reasons why some people flocked to them.

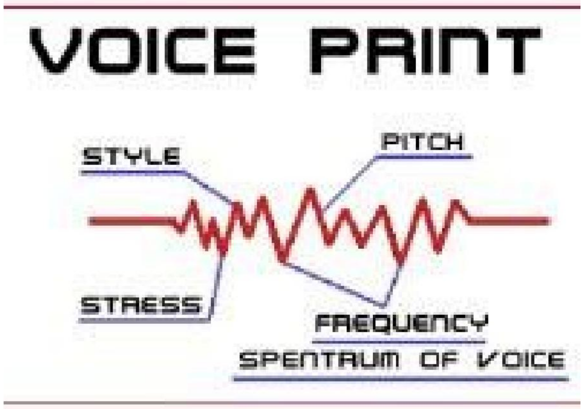
However, the issue of smart lock security was one that gradually made its way to the foreground of the conversation. Smart locks made little architectural improvements to the basic design and components of traditional locks, so they each essentially start out on the same security threshold (in most cases). In this sense, most people would think that their smart locks are better than their traditional locks because they are being afforded the same level of security with added features, but this isn’t always the case.

Most smart locks will work with an existing deadbolt, which does imply that they are offering a much more secure lock than if you were to use a Euro Cylinder lock on your front door. Though this might be better, there is a drawback to this. Due to the specific nature in which smart locks are designed, it is hard to make additions to them. A perfect example is the August Smart Lock, which can only work with thumb turn deadbolts and will not work with double cylinder deadbolts. Another example is the Kevo Kwikset, which comes with its own hardware (lock cylinder, interior set up, etc.) and is meant to replace whatever hardware a homeowner had in place.

II. METHODOLOGY

Optical fingerprint sensor can be used, as it captures a photo of our finger ridges since ridges and patterns are very important in the analysis of fingerprints as no two fingerprints have been shown to be identical, and it uses certain algorithms to match it with the stored data, connections can be done for the power, data as well as with hardware bolt to lock & unlock whenever needed. Desired finger impressions can be enrolled in Scanner Module and stored in the IC registers of the Microcontroller. With the interfacing method, fingerprints can be used to create secure and impenetrable lock. Interfacing can be done by developing communication between Microcontroller and Interface. Motors are used for locking and unlocking the door.

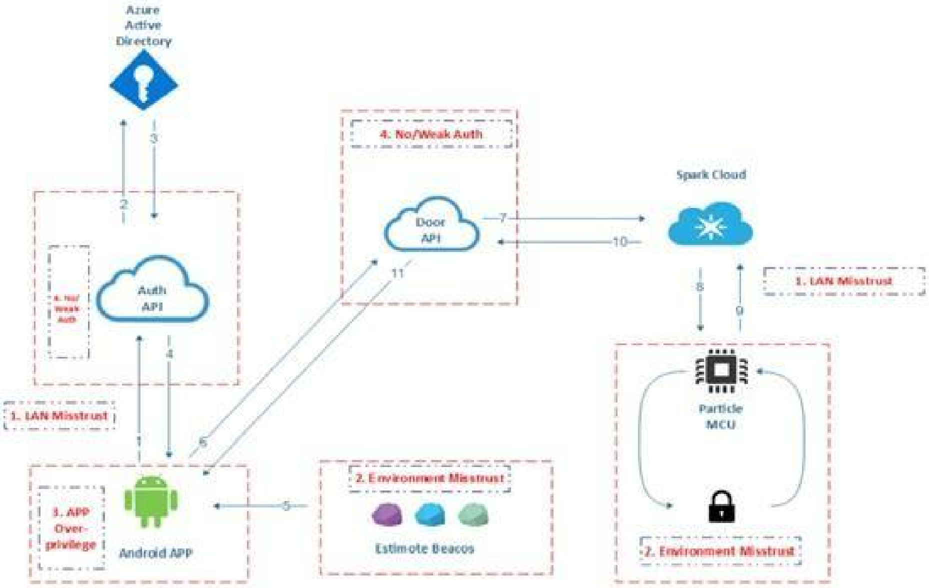
However, if an unauthorized person tries to breach lock, beeping sound takes place after number of trials are expired, also designated app will send a continuous pop-up to registered user in the app as well as leave a SMS, incase user is offline. This Pop-Up Notification will be having an option, if user wants to lock the door/system with high level security which will be delivered via app as well as SMS(can be enabled using desired numbers, for example 1,2,etc). This high level security will be triggering voice recognition system to take place. Voice recognition will take voice input from the user whose identity needs to be stored in the device. The voiceprint is made with the use of software that splits voice input statement into various frequencies. The prints are stored in databases to identify later and acknowledge users.



Adding this feature will add security, as system now can be only unlocked when user uses finger impression as well as input voice. However, if someone tries to harm microphone or finger impression sensor, system will send an appropriate message accordingly. Incase, internal parts are damaged system can be unlocked using CustomerCare Service where user has to provide their product's primary key (different for everyone), which will allow executive to unlock the system. As earlier mentioned, locking system will not be only restricted for the main door but it will have different product(smart padlock, smart sliding lock, etc) according to price range and user's need.

III. ANDROID BASED APPLICATION

An extensive and user friendly Android application has been developed to control and monitor the status of biometric door locks. The communication between application and server was achieved by Apache HTTP Client. For data exchange between client and server JSON was employed. The user has to get registered to the device before using the application, providing personal details. On a single android phone only one user can be registered though one user can login on multiple phones. After successful registration and login, user can insert, delete or edit door locks along with the desired features to be attached with each door (doorbell detection, door knock detection, suspicious person). After login user selects a door and views the activity tab of that door with images of visitors and time of arrival, action tab on which he/she can see all the unlocking actions performed by users of that door, status of different doors (open/closed) and unlock the door by putting his/her finger on the fingerprint sensor of the door if it fails the number of trials then it will give a notification on the app and then the user will immediately receive a notification that someone is trying to Breach The lock System with an option if they want to enhance security, if user allows that option, the lock will immediately turn on voice recognition and will unlock only when user Speaks as well as Place Finger on the sensor. The user guides of how to use application and how to use the device are also available. Moreover a single android device can make only one account on server fortifying the security. Notification is received on android application whenever any activity is occurred or action is performed. On opening notification, application allows user to unlock door after biometric or voice is verified. The Purpose of Collecting Contact Number & mail id is when user is offline, user will receive a text message on their given phone number as well as on given mail id. In Software update, we can introduce the feature of adding contact info of neighbors as well, so that neighbors can also receive pop-up notification, if user wishes to inform them.



Android Application asks for authentication by sending username and password via HTTPS.

"Auth API" ask for an access token from Azure AD with provided user credentials, resourceID, and clientID.

If the information sent with the request is valid the Azure AD responds with an access token valid for 2 hours.

The token is sent back to the Android Application via HTTPS. The Android client can now make authenticated calls to the Door API.

The Android application will start listening for registered beacons. When a Beacon transmission is received, the application will confirm that the beacons are from a valid source.

The Android will request to open the door if the beacon(or biometric /voice) validation is successful. Access token and the function name is provided in the HTTPS call.

The door will send a new HTTPS request to the particle if the received request is authenticated and authorized. The request to Spark Cloud will contain the unique access token and deviceID for the Particle device.

Spark will send the specific function call (in this case "open door") to the device with the correct deviceID.

The Photon device will return a specific value of the function called was executed correctly or not.

Spark Cloud will send an HTTPS response back to door API containing information about the status of the request.

Door API sends a response back to Android telling the application if the request was successful or not.

DOI: 10.48175/568

What is REST API?

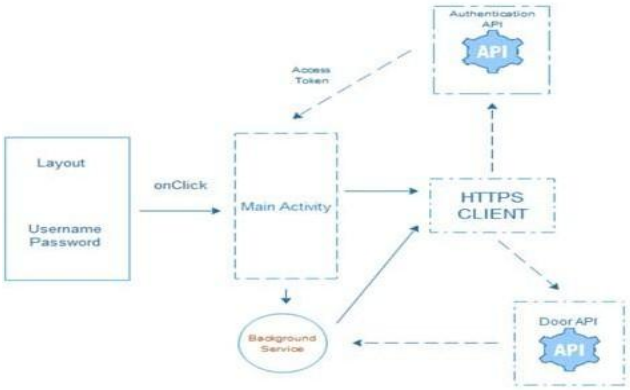
Representational state transfer technology (REST) is a software architectural approach and procedure used for the goal of communication in web-based services. REST is an API that uses HTTP requests to get, post, put and delete data. This API uses HTTP paradigms. REST API uses GET function to regain a resource; PUT function to change the nature of/update a resource, which can be a block of information or a file; POST function to create a resource and DELETE function to remove it. This API structure is important to minimize the coupling between the client and server components in a distributed application. REST is an interface between systems using HTTP to obtain data and generate operations on these data in all possible formats (e.g XML and JSON).

Communicating to and from the REST API

To make different calls via the internet can be dangerous from a security perspective but is in our cause definitely necessary. The Particle door device needs to be fed different tasks as door unlocking to be able to perform in a wanted manner. When transmitting data via the web the sender has no control over which path it chooses takes to reach the receiver. This means that nodes on the internet can intercept the data and read it if it is not encrypted in some kind of way. The most standard protocol for receiving or requesting data over the web is HTTP (Hypertext Transfer Protocol). The standard HTTP protocol comes in various forms and has all the functionality needed for calling our web APIs. However, there is one major problem; the HTTP sends data via plain text. This is a large issue as anyone interacting the HTTP request on its path the response can easily read or intercept data without us ever knowing. This will make all the security measures we implement useless and unnecessary as an attacker simply can read all the communication within the system. extracting sensitive data as username, passwords, or tokens. Fortunately, there is a simple solution to this problem called SSL (Secure Sockets Layer). By combining these two protocols you get a safe and secure protocol with all the functionality of the HTTP, this protocol is called HTTPS. HTTPS relies on asymmetric and symmetric cryptography and all the data send between two nodes a completely encrypted.

Application Overview

The SDL app will be requiring the user to enter the login credentials (username, password). Clicking on the login button will activate the onClick() method that in turn will go to our MainActivity and trigger an HTTPS request through the HTTPS client. The credentials will be sent in a scrambled message with an agreed code between the sender and the receiver (Authenticate API in our case) and transferred on a Secure Sockets Layer where no one can read the message. The user's credentials are authenticated in API, when the Authentication process is completed and succeed, the Access Token is sent back to the MainActivity in the SDL app. At this point, the app is ready to start the Background service and begin to scan for beacons. When a valid beacon is found, an authenticated request is sent (containing the acquired Access Token) through the HTTPS client to the Door API where the validity of the token is determined. A proper response is then sent from the Door API telling the application if the request was successful.



App Prototype Link https://thegraphicgallery0.wixsite.com/website

IV. RESULT

- As a conclusion, Now keys can be optional! also locking systems will be more secured.
- The lock device will be available in number of variants & customisation according to price range as well as consumer's needs.
- Purpose to Introduce this Smart Lock is to give more security to the user which will not bound only to specific doors.
- Breaching the lock will automatically lead to activation of high security(Voice and Finger Impression)
- Due to this technology high security will be assured in Cabinates, Lock Safe's, Sliding Wardrobes, Padlocks, etc.
- Designated app and Contact Registraion will keep you notified in every situation.
- User Friendly App, which will allow user to manage their multiple locking systems through one app.
- Each Locking Product will come with Primary Id which will be known to user and will help to unlock their locking system via co-ordinating with 24x7 Customer Care Service.
- Minimise the breaching of locks as Neighbours can be notified as per user's virtue.
- User can always add, delete and update Voice Prints, as well Finger Impressions through their app.
- So Many Options to Lock and Unlock with High Level of Security

V. ACKNOWLEDGMENT

This paper and the research behind it would not have been possible without my enthusiastic team, and our mentor, Prof. Deepali Sonawane, her guidance, knowledge and attention towards detailing have been an inspiration and kept our work on the track. Also, my colleagues Vaibhav More and Aryan Rathod contributed their valuable support and knowledge to bring most out of this topic. I will also be grateful for the comments offered by anonymous peer reviewers at National Research Conference. The generosity and expertise of one and all will definitely encourage me to do more better in future. We are also immensely grateful for the comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of esteemed persons.

REFERENCES

[1]. https://www.diva-portal.org/smash/get/diva2:1216681/FULLTEXT01.pdf

[2]. https://www.claysys.com/blog/voice-biometric-authentication/

[3]. Smart Door Lock Using Fingerprint Sensor Piash Paul, Md. Abdullah Al Achib, Hazrat Sauda Hossain, Md. Kaviul Hossain