Smart Door Using Biometric NFC Band and OTP Based Methods

Varasiddhi Jayasuryaa Govindraj, Yashwanth P.V., Srinidhi V. Bhat, T.K. Ramesh
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru
Amrita Vishwa Vidyapeetham, India.

***Abstract*— In this technologically evolving era, with the transition towards a wireless world, security plays a vital role in ensuring the safety. Over the years various methods have been proposed by researchers across the globe which have proven to be successful but have lacked in areas such as security and authentication time. This paper presents an innovative design for a Smart door with the aid of a biometric NFC band and OTP authentication methods which would provide secure and easy access to our homes. Our idea brings forth the opportunity to mitigate the issues faced by these systems by reducing authentication time with the help of a biometric fingerprint sensor and adds an extra layer of security using the help of a local server to generate OTP authentication. This implementation has shown better results and higher performance rate than existing methods.**

Keywords: Arduino, Biometric, OTP, NFC, RFID, GSM Module.

I. Introduction

Since the advent of mankind, we have always looked for ways to simplify our day-day activities however, this compromises on security. As we are living in a digitalized society, privacy and security comes of at most importance. Every system designed is incorporated with the loophole through which security is compromised. We have seen that Home Automation has become a significant part in the smart home transformation [1] and are in now in trend. As more people integrate smart appliances into their living spaces, the necessity to enhance the security of such an integration becomes more essential.

Near-Field Communication (NFC) is a set of communication protocols that enable devices to transmit information between them wirelessly. NFC is used in contactless payments, smart tags, wireless keys, etc. NFC being a versatile tool can be incorporated in a variety of devices such as Debit/Credit cards, mobile phones, etc. Although the use of NFC is ubiquitous, they are prone to many security threats such as theft, hacking, etc. The significance of Home Automation is the security and ease of use. The current implementations of a Smart Door lack in ease of use and security. Often the implementations compromise on either security or access time.

To overcome these security threats and access issues, our paper presents an innovative and economical solution to this problem by using 2-level security comprising of a biometric verification and a verified OTP access. The use of the NFC band is to authenticate the user before unlocking the door. The OTP access tool will be used when a guest is requiring access to the house. The remaining document is structured as follows. Section II talks about the literature survey of NFC security, Section III talks about the functionality, the algorithm and working are explained in Sections IV and V, and future scope and conclusion is explained in Sections VI and VII.

II. Related Work

There has been a lot of work done on NFC/RFID technology to improve the simplicity of our lives. A concept design, both innovative and ingenious has been presented by R.M. Nipuna Deelaka Ranasinghe [2] by illustrating a device that uses fingerprint authentication to functions as an RFID or NFC tag. The basic principle is that the input/output of an RF signal is obtained only for verified fingerprints. The NFC/RFID device with fingerprint authentication contains data encryption along with a few more such facilities as its supporting properties. Security threats such as hacking hardware or software, malware, etc. are prevented from the device as the isolated system does not contain back doors. But the major drawback is that the NFC device designed here is comparatively overpriced since the sensors used (fingerprint sensor, display, charge port) are costly resulting in increase of manufacturing cost of the device.

A scheme is brought forward by Geetha Govindan [3] wherein RFID, Biometric and Smart Messaging are used as the essential tools to present security management techniques in real time. Biometric Machines are used to control entry of registered staff through their RFID cards as well as to oversee entry to restricted areas. Successful comparison of the staff duty roster timings with the biometric credentials provided will unlock the door through the relay in the biometric reader. Oracle 10g Database is used for registering staff details, entry/ exit time in order to process attendance. An unapproved attempt to open the door activates the GSM modem to sends Notification alert to the security incharge person's mobile

phones and to Duty in Charge's mobile phones referring from the database while simultaneously recording the illegal attempt by the particular person in the database. Biometric reader interface is developed using Software Development Kit (SDK), GSM modem is interfaced through AT commands and Smart Card programming & Oracle programming is done for server interface. Since they are using contactless card for biometric verification anyone who is having this card can access through the security system which means the security system is more vulnerable to attacks.

Hussani Habibu focuses on the access control systems which breaks the access to a secured premise or assured safety devices only to approved personnel [4]. This idea involves a biometric access control developed with additional feasibility i.e. including or terminating users and constant vigilance on the system's operation through a GSM mobile. The proprietor device sends SMS adjures to the system to enable required modes of operations and to include or terminate users of the logic. Thus, the system can toil independently and as condemned by the proprietor. Major drawback in this paper is that, the whole working model depends on the network connectivity of GSM module. Bad and inconstant network will affect the communication in between the administrator and the model, and this may lead to utmost burden to the mode of operation.

Ezzaldeen Edwan outlines an unconventional technological solution to the problem of utilizing conventional mechanical keys for door lock system [5]. The basic objective of the work is to model and execute the use of system which uses automated keys for the home security purposes. In this system, keys can be kept in a key cabinet, which can be locked and opened automatically. For this NFC technology which is widely present in all the latest mobile handset technology is used to identify each and every key. Keys can be used by the owners with the help of a NFC identification tag given to them so that the theft of keys can be avoided. The main drawback of this model is that once the RFID identification tags given to the owners are lost due to their size he/she cannot have access to the keys which creates a whole lot of problem for the owners to lock their respective houses while going out or to unlock when coming from out.

III. FUNCTIONALITY

In our paper, we offer two methods,

1. NFC Band (Registered Members)
2. OTP (For guest user)

We propose to use an Arduino Uno paired with a GSM Module and a NFC reader attached to the door (refer Figure. 1.). For the NFC band, we plan to use Arduino Mini connected with a fingerprint sensor and a NFC Tag. We plan to use GT-511C3 fingerprint sensor with the UART protocol and SmartFinger 3.0 Algorithm. The previous methods use fingerprint sensors that are not very efficient in terms of the authentication time. This sensor has a very fast authentication time and can also store up to 200 fingerprints in its database. Also, since the Arduino itself is generating the OTP, we mitigate the time lag faced when the OTP is generated by a server and sent to the guest user's mobile phone.

The NFC Band [6] with Biometric authentication is embedded with a fingerprint sensor, on which by placing the registered user's finger on the sensor the Biometric authentication is carried out (refer Figure. 2.). A screen that is embedded in the band located is used for displaying information regarding the band charge status, the status of the user authentication. OTP authentication is used when the guest access is to be provided. Smart lock with a screen and a keypad is the vital part of the smart door system where a guest needs to enter his/her mobile number which will be sent to the owner's NFC band. The owner receives an SMS from the Arduino via a GSM Module which will provide the phone number that the guest had previously entered. The owner then verifies the mobile number of the guest and Sends a positive acknowledgment. The guest then receives the OTP from the Arduino via the GSM module and enters it into the Keypad for entry into the house. In the next section, we give the detailed protocol for the above-mentioned methods.

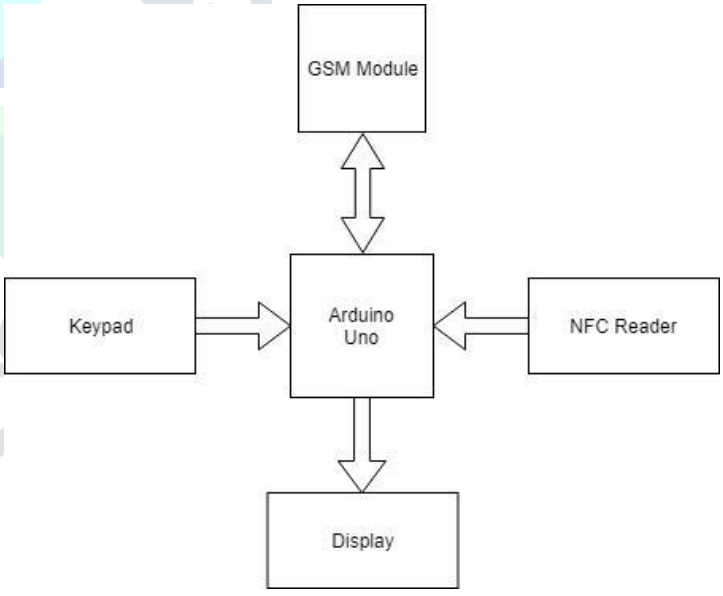

Figure. 1. Block Diagram of Smart Door

Figure. 2. Block Diagram of NFC Band

1. NFC PROTOCOL:

Step 1: The user must be near the door to tap the NFC band for access into the home.

Step 2: User must scan his fingerprint using the fingerprint sensor placed on the NFC band.

Step 3: Once the fingerprint has been verified, the user can tap the NFC band on the NFC reader of the door for entry into the house.

A. Biometric Authentication

The NFC band is embedded with a fingerprint sensor. The NFC band has a storage element which will store the owner's fingerprint. The fingerprint sensor controls the functionality of the NFC band and will only activate it once the user's fingerprint matches that of its owner's. When the owner wishes to enter the home, he must scan his fingerprint using the biometric sensor on the band. Once the sensor identifies the owner, it will activate the NFC band. The user can then tap the band on the NFC reader on the smart lock to gain access into the house [7].

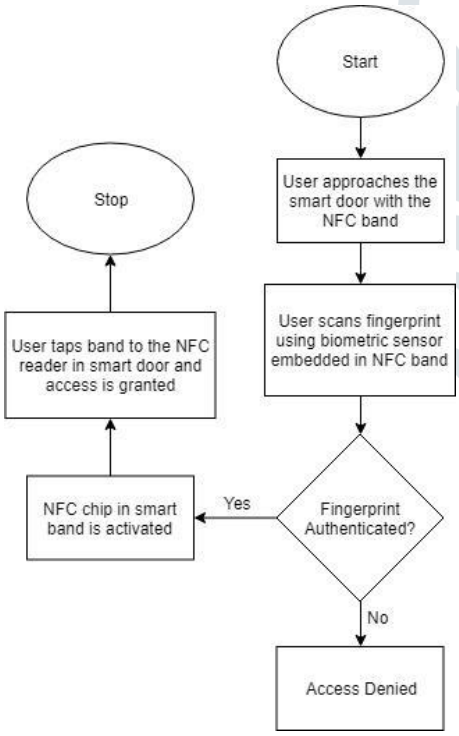

Figure. 3. Flowchart of NFC-Based Authentication

2. OTP PROTOCOL:

Step 1: The guest must enter his mobile number using the Keypad on the door.

Step 2: The Arduino-GSM system sends an SMS to the owner of the house for granting access into the house for the guest.

Step 3: The owner approves of the guest by sending a "YES" confirmation back to the Arduino-GSM system.

Step 4: The Arduino then generates a random OTP and sends it to the guest's mobile number via the GSM Module.

Step 5: The guest enters the OTP onto the keypad and is granted entry into the house.

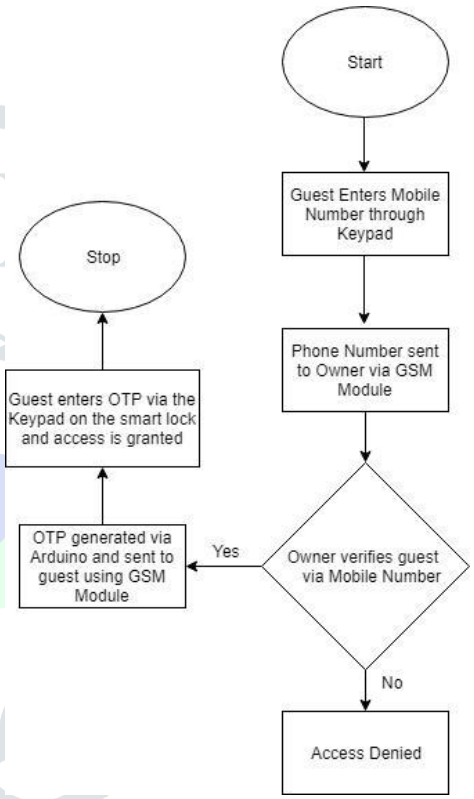

Figure. 4. Flowchart of OTP-Based Authentication

B. OTP Authentication

The smart lock is embedded with a screen and a keypad. An Arduino interfaced with a GSM Module is integrated in the smart lock [5]. When a guest requires access into the house, he must enter his mobile number into the lock with the help of the keypad. A SMS is then sent to the Owner's mobile with the help of GSM module [8] informing the owner of the guest. The owner, if he decides to allow the guest to enter the house, accepts the entry by sending a "YES" SMS back to the smart lock. The Smart Lock then sends an OTP to the guest's mobile number. Once the guest enters the OTP, he is granted access into the home.

The mutual working of these two authentication methods brings about an efficient secure system. This two-level security ensures the easy fortified access to the home for both the owner as well as for the guest.

Table. 1. Comparison of Proposed Model with existing NFC Based Models

Characteristics	NFC based smart device (Previous model)	NFC based smart band (Proposed model)
User Authentication	It didn't have a method to authenticate user.	A biometric sensor is implemented in the smart band to identify the user.
Security	Owner is unable to give remote access to guest securely.	An OTP based system is present in proposed model where the guest enters his/her mobile number and the owner has the ability to grant access to the guest to enter the house.
Speed	For models having authentication, authentication time was high.	In this model we will be using an efficient biometric module which takes around 3-5ms of time to authenticate user's fingerprint.
Robustness	Robustness of these systems is relatively less.	Robustness of our model is more due to its 2-level security system.

IV. Future Scope

We can further extend this project by adding facial recognition and speech recognition [8] to further build on the biometric [9] side of security. We can also install a camera which can be used to track the activities of unknown people and intruders. A smoke detector can also be paired with the Smart lock to detect any accidental fires and alert the owner of its presence via SMS. Using this model, we can also develop a smart parking ticketing system with the help of NFC tags [10].

V. Conclusion

The use of NFC/RFID tags comes with the risk of security. Previous implementations of Smart doors have had to sacrifice in security and ease of access. To overcome these issues, our model implementation integrates an NFC band [9] with a fingerprint sensor to verify the owner before unlocking. We have also added an additional layer of security [3] in form of an OTP access system for guest entry. Therefore, these two methods of security eliminate many potential risks such as theft, hacking, duplication, etc. Thus, the use of this system brings forth the opportunity for a better secure home without compromising on security and access time which makes the day to day life of the user much simpler.

References

[1] D. Vishal, H. S. Afaque, H. Bhardawaj and T. K. Ramesh, "IoT-driven road safety system," 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Mysuru, 2017, pp. 1-5.

[2] R. M. N. Deelaka Ranasinghe and G. Z. Yu, "RFID/NFC device with embedded fingerprint authentication system," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2017, pp. 266-269.

[3] G. Govindan, S. K. Balakrishnan, R. L. Ratheendran and S. K. Sivadasan, "Real time security management using RFID, Biometric and Smart Messages," 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, Hong Kong, 2009, pp. 282-285.

[4] Hussaini Habib, Adamu Murtala Zungeru, Ajagun Abimbola Susan, Ijemaru Gerald Kelechi, Oresanya Babajide Oluwatosin, "Design of a GSM-Based Biometric Access Control System", Control Theory and Informatics Vol.4, No.8, 2014.

[5] E. Edwan, A. Shaheen and A. Alloh, "Assets and Keys Management System Using NFC Technology," 2018 International Conference on Promising Electronic Technologies (ICPET), Deir El-Balah, 2018, pp. 8-12.

[6] O. Bindroo, K. Saxena and S. K. Khatri, "A wearable NFC wristband for remote home automation system," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-6.

[7] R. L. Jorda et al., "Comparative Evaluation of NFC Tags for the NFC-Controlled Door Lock with Automated Circuit Breaker," 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), Baguio City, Philippines, 2018, pp. 1-6.

[8] D. Sunehra and V. Tejaswi, "Implementation of speech-based home automation system using Bluetooth and GSM," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016, pp. 807-813.

[9] S. Vhaduri and C. Poellabauer, "Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3116-3125, Dec. 2019.

[10] D. Kanteti, D. V. S. Srikar and T. K. Ramesh, "Intelligent smart parking algorithm," 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bangalore, 2017, pp. 1018-1022.