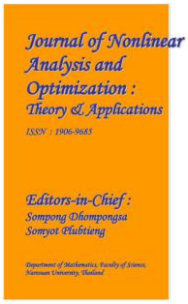
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**



AN ADVANCED LOCK SYSTEM USING NOVEL SECURITY INTEGRATION

Dr. M. Chiranjivi1, K. Suresh2, G. Chandranshekar3, M. Siddarth4
1,2,3 Associate Professor, Department of EEE, Hyderabad Institute of Technology and Management, Hyderabad, Telangana, India
,3 Associate Professor, Department of CSE, Hyderabad Institute of Technology and Management, Hyderabad, Telangana, India
4 Assistant Professor, Department of EEE, Hyderabad Institute of Technology and Management, Hyderabad, Telangana, India
1chiranjivimadduluri@gmail.com, 2sureshk.eee@hitam.org, 3chandrashekarg.mca@hitam.org, 4siddartham.eee@hitam.org

Abstract –
In general, the traditional or smart locks are single staged as well as external visible device so there is a maximum chance for trespasser to damage (Physical or Hacking) the locker system. The proposed paper is a prototype of Novel Smart Lock device, which is a high secured compact device with mandatory of Internal (Secondary Stage) and External (Primary Stage) security verification. The Primary Stage is having a Primary Door (sliding door) with its operating security modules visible for external access and the Secondary Stage is having a Main Door along with its smart security verifying modules kept internal to the Primary Door. To design this model RFID module and Bluetooth HC05 modules are used as Primary Stage Security System (PSSS), Fingerprint Scanner and Voice Recognition modules are used as Secondary Stage Security System (SSSS). However, the Primary Door is accessed by a proper Authentication of any one module in the PSSS and the Main Door is accessed by its successful Authorization of any one module in the SSSS. Therefore, when we want to access the Main Door, we must pass our credentials at Primary Stage as well as at Secondary Stage, then only we can access the actual door lock system. Hence the proposed solution is a high secured door lock device, and it completely controls unauthorized access of trespassers or hackers at its under limits.
Keywords: Primary Door, Main Door, Authentication, Authorization, Primary Stage Security System, Secondary Stage Security System

Introduction

In this present generation, everything is digitalized and many of us are getting used to work with smart appliances rather than traditional things as they work with greater efficiency, time management, low cost, appearance, simplicity, and ease of use. However, the safety applications like digital locker, electronic lock devices and smart lockers for domestic, commercial and bank purposes having advanced technology of Wireless Fidelity (Wi-Fi),Internet of Things (IoT), RFID, Finger Print Scanner, ZigBee, GSM, Bluetooth HC05 and Smart Phone (android app) paired are available in the market, but in security point of view no device is trustful as they are facing so many security issues like digital hacking, security code (password) decoding, technology (data) misuse, spoofing, trapping by hackers or burglars and so on. Hence more research is needed in the development phase of smart safety device, in this connection we noticed that the security devices currently available are visible for external people, which causes to allow the hackers or burglars for unauthorized access.

The proposed paper is an extension of work originally presented in 2019 global conference for advancement in technology [1] and the existing solution is a kind of smart lock device which uses

smart verification at each stage, but it seems limited security at secondary stage verification. In general, we have carried, and non-carried type of keys used in the digital or smart lock devices; RFID and Bluetooth HC05 with Android Mobile App come under the category of carried, and Fingerprint Scanner, Voice Command based come under the category of non-carried keys. So, the proposed solution focusses on providing an additional feature of voice commands to the existing solution to make the safety device stronger in all aspects of control of unauthorised access in door lock operation. The remainder of the paper is organized as follows; section-2 consists of related work, section-3 implements the methodology, section-4 provides the design of the system, section-5 shows experimental results and finally the section-6 concludes the paper.

Related Work

Authors J. Pacheco and K. Miranda presented a prototype system for home automation based on a digital door lock with Near-Field Communication (NFC) technology and the Arduino Mega board,which operates on card emulation mode and it allows the user to interact with an NFC reader through their NFC enabled mobile [2],the authors in paper [3] also have the same approach but these systems doesn't allow guests without having NFC mobile card and unfortunately, if we lose the NFC mobile we cannot access the door. Authors proposed a model of intelligent door locking system, that has an Application (App) for android based smartphones with the ability to recognise image based face recognition using OpenCV library and if not matched with the database results, they provide another way of RFID along with digital password based security system to access the door lock [4], but the solution depends on alternate methods as the face recognition has difficulties with finding face recognition even though the user is an authorized.

In [5], the author proposes a system of Wi-Fi for the internet connectivity between Node-MCU and the cloud server IFTTT and Motion detection sensor to detect the moving object. If any moving object is sensed it will send the alert to user through IFTTT and Adafruit IO, then the owner of the house alerts whether the moving object is authorized or not ,here all the communication is done through the MQTT protocol. In paper [6], authors use an android mobile application and HC-05 Bluetooth device, firebase database to register the app with the database; when the devices are paired and credentials are matched with the data base results the door lock will be accessed, however the same approach is followed in the paper[7,8,9,10].These system will work with mobile app of internet connectivity and database management system, so these are expensive and will not work out for remote location areas as well as for low internet connectivity places.

In the papers [11,12], the author researchers proposed a two factor authentication of RFID and OTP feedback system , when user want to access the lock system by placing RFID tag on to the reader, an encryption code will be generated and is validated at its interconnected cloud server , if the code is matched, an OTP will be sent to the corresponding user for second stage verification of OTP validation by the android app of user, and if this OTP is also verified, then the door lock will be accessed, a similar work is proposed by authors in [13] with some changes of using Wi-Fi technology. So, this kind of methodology takes more time to react, and it requires frequent database maintenance.

The authors in papers [14,15], proposed a ZigBee technology this contains a ZigBee and a phone pair which is named as ZigBee-tag used for door lock access by making communication between human detection sensor module and digital door lock when an authorized person arrives at the door, since the ZigBee requires a proper pair of transmitter and receiver modules, if a module is damaged, the total system is damaged. The inventors in paper [16] have a five-pin secret password to lock and unlock the door, when something goes wrong with the password, the GSM which is already existing in the system alerts the owner, Paper [17] also have the same concept of password-based access but GSM based is a time taken process and it is completely operated on a network basis. Authors in paper [18], controls the door lock by the voice command at his mobile voice recognition application through Bluetooth technology and it always requires a same voice frequency range which is a kind of drawback.

In this paper, we present a combination of carried and non-carried key approach, which is a non-internet connectivity based as well as no protocol-based communication (wireless) and it is an independent of database support.

Methodology

In this section, construction of each stage is described: that is primary stage security system and secondary stage security system along with its sensors and controller's involvement.

Primary Stage Security System

It is an externally accessed primary door operation, which holds the entire secondary stage security system underneath the primary door. As shown in the Figure 1 of schematic diagram, the system is constructed with an Arduino controller unit, two modes of RFID and Bluetooth based security modules along with a primary door operating motor.

3.1.1. Arduino Uno Micro Controller Unit

The Arduino uno is an 8bit AVR micro controller board developed on ATmega328P data sheets [19] operated on DC 5V,16Mhz frequency with of 14 digital I/O and 6 analog pins, by default some digital pins are configured for multipurpose, we can utilize them for I/O as well as for external peripheral communication. As shown in the Figure1, the RFID reader and Bluetooth HC05 modules are connected as an input device to the Arduino by using their specified communication protocol and a DC 5v motor is connected as an output device through a L293d current driver to operate the primary door (sliding door).

3.1.2. RFID Security Mode

The MFRC522 RFID module is used as one of the security modes of primary stage security system, it is available as RFID transceiver module and its Tag. As shown in the Figure1, the reader module communicates by the SPI protocol to the Arduino digital I/O pins of 10,11,12 and 13 at the frequency range of 13.56MHz, however the RFID tag is a passive tag which includes a microchip for storing unique identification codes and an antenna to activate the microchip [20].

3.1.3. Bluetooth Security Mode

The Bluetooth security mode is another mode of primary stage security system, it is available of Bluetooth HC05 module and its supporting Bluetooth android mobile phone application [21]. As shown in the Figure1, the Bluetooth HC05 is connected and communicated to the Arduino controller using USBTTL serial communication protocol with a baud rate of 9600, Bluetooth device accepts the commands of its paired device of android mobile app with a strong secret password in between the range of 0000 to 9999.

3.1.4. Primary Door

The primary door is also called as a sliding door which is fitted to a rugged box to make sliding actions with the help of a DC 5v electromechanical motor (mini motor) and is operated when input sensors activate the controller unit. As shown in the Figure1, the Arduino controller and motors are connected via a L293D current driver to make the stable operation of the motor as the controller unit rated current is limited to 30-40mA per each digital I/O pin.

Secondary Stage Security System

As shown in the schematic diagram of Figure 2, the secondary stage security system comprises of an Arduino mega controller, fingerprint scanner mode, voice recognition mode and linear actuator motor to access its main door operation.

3.2.1. Arduino Mega Controller Unit

The Arduino mega 2560 is a micro controller board developed on ATmeg2560 data sheets. Compared to the Arduino uno, it is a similar board having more digital I/O pins and serial communication ports. As shown in the Figure 2, the LCD unit, linear actuator motors are connected as output devices to the digital I/O pins and voice command control system, fingerprint scanner systems are connected via TTL UART serial communication ports as an input device.

3.2.2. Voice Recognition Mode

Elechouse V3 Voice Recognition Module is connected to the Arduino with TTL UART serial communication protocol, which can recognize 80 unique voice command but in our model development purpose, we have trained and recorded up to three commands as it is enough for the application requirement.

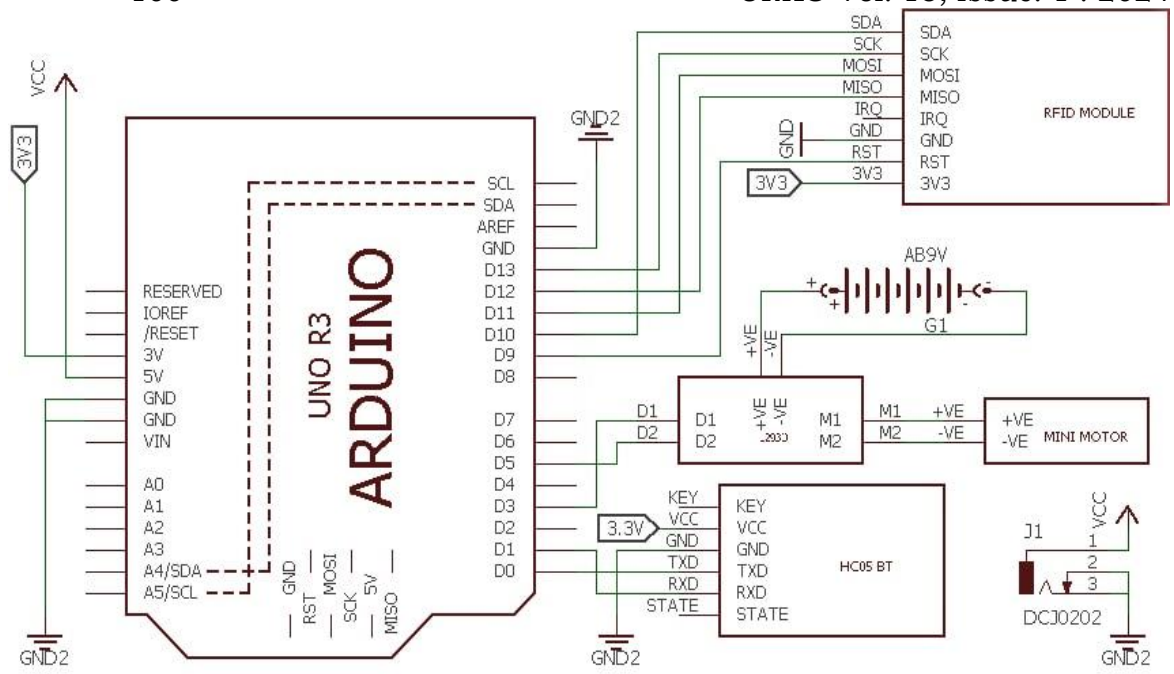


Figure 1: Schematic Diagram of Primary Stage Security System

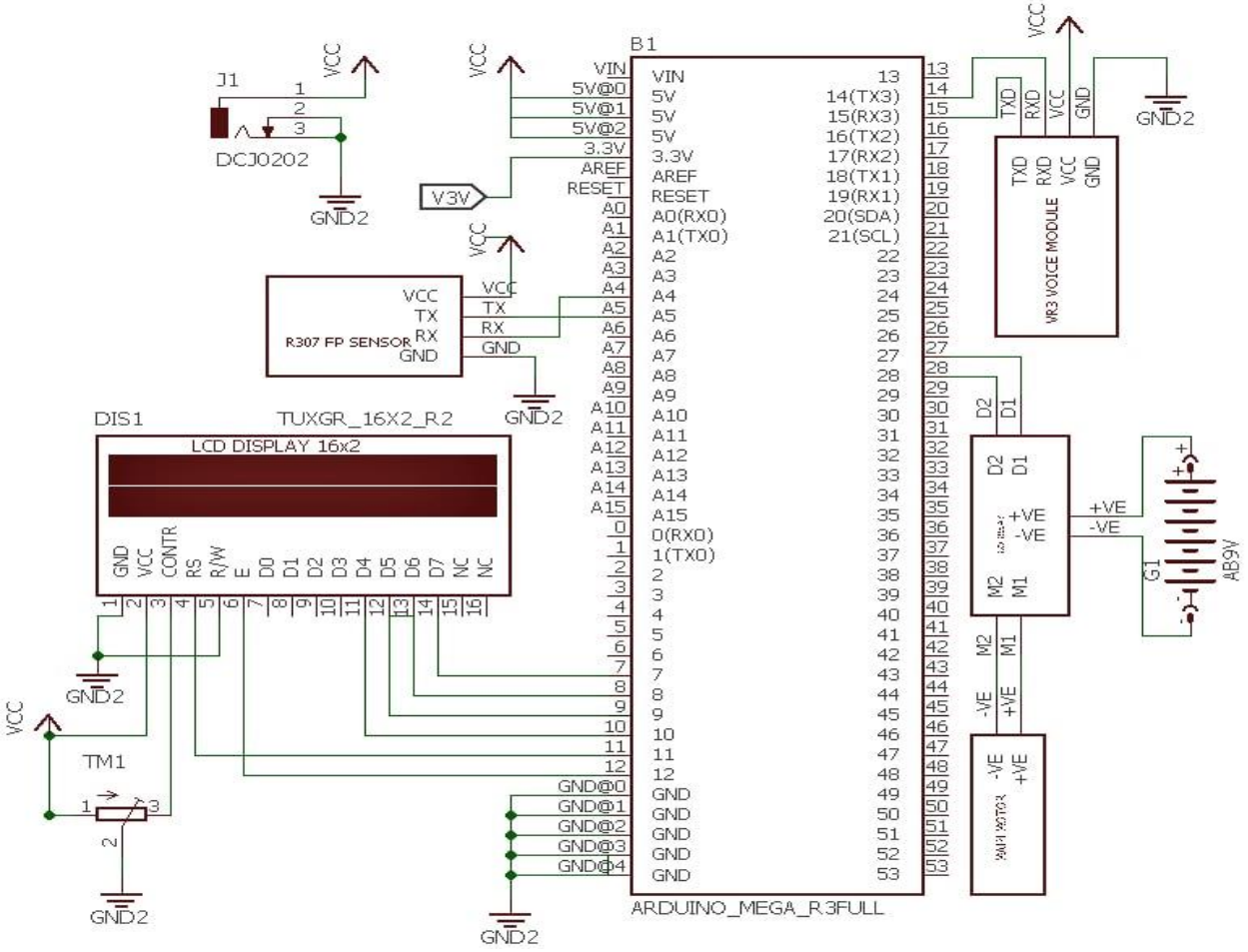


Figure 2: Schematic Diagram of Secondary Stage Security System

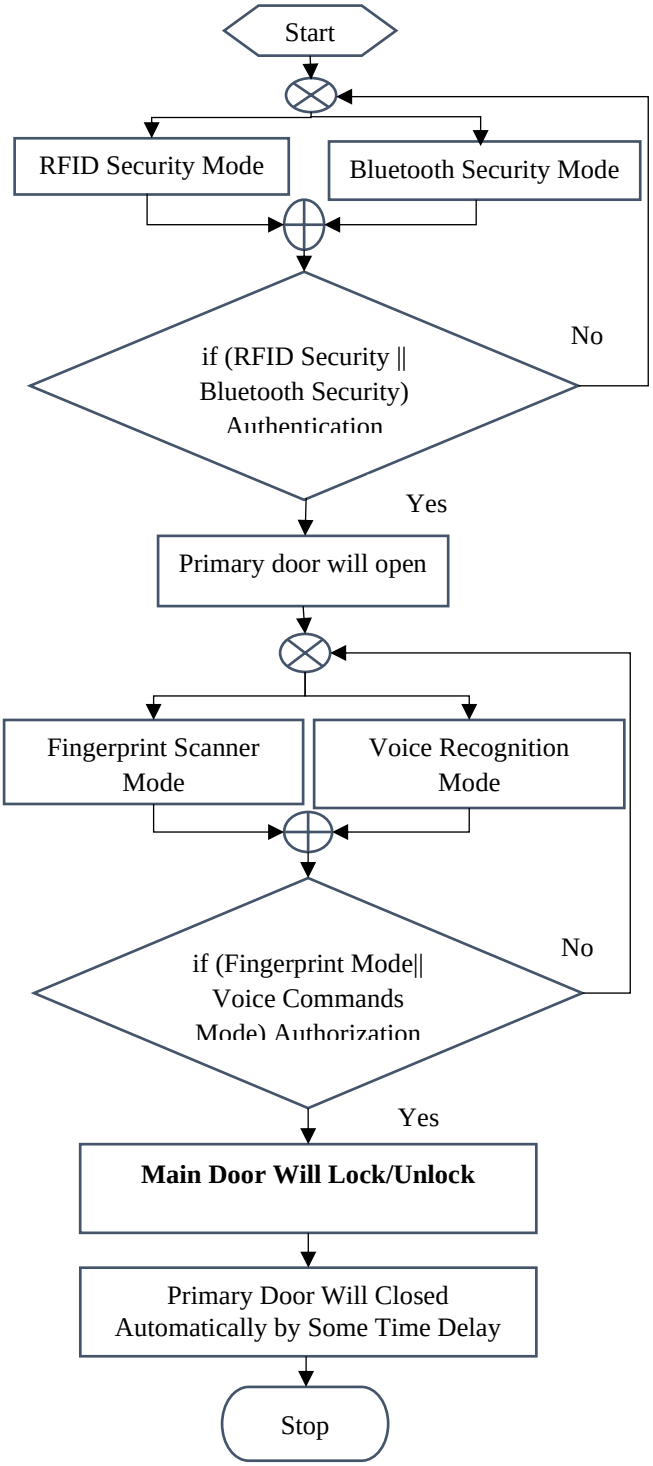


Figure 3: Flow Chart for Main Door Access

3.2.3. Fingerprint Scanner Mode

R305 fingerprint scanner system is connected to the controller unit through the TTL UART serial communication protocol, which can support independent fingerprint registration, fingerprint comparison and fingerprint searching functions [22]. Here we have registered up to three user fingerprints and stored in the sensor memory in the form of image packets.

3.2.4. Main Door

A DC 12v linear actuator motor is connected to the controller via a12v DC relay to operate the main door, which kept inside to the main door as it is an internal operation of the main door access and it is a high torque motor, which moves upwards and downwards in direction instead of clockwise and anti-clockwise direction.

Design of the System

The design of the proposed system is shown in the Figure 3 of flowchart as we know that the door lock access involves lock and unlock modes, thus the system also uses two modes operation: such as Main Door Lock and Main Door Unlock modes.

Main Door Lock Mode

In Main Door Lock Mode: the proposed system uses an internal locking mechanism, which is operated by a proper Authorization of anyone of its secondary stage security verifying modules but before accessing this stage user must access his primary door by its authentication security modules called primary stage security system.

4.2. Main Door Unlock Mode

In Main Door Unlock Mode: user will unlock the internal lock mechanism of linear actuator motor from the outside of door and before to reach this main door, user must pass his credentials at primary stage Authentication and then at secondary stage Authorization, then only the user can access his main door unlock mode.

Experimental Setup and Hardware Results

The external view of smart lock device with multistage-multimode security integration is as shown in the image of Figure 4. hardware setup of proposed methodology.

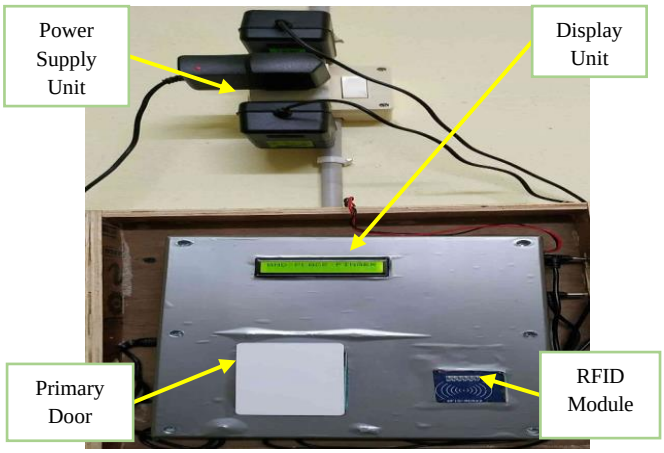


Figure 4: Hardware Setup of the Proposed Methodology

As we already discussed in the previous sections, there are four modes of security modules involved in the operation of locking/unlocking of primary door/main door and the operation is stated as in the tables 1 & 2.

Table 1: Primary Door Lock/Unlock

Mode of Operation	RFID Security Mode	Bluetooth HC05 Security Mode
Primary Door Unlock	**Verified**	Not used
	Not used	**Verified**
Primary Door Lock	No need to lock it will be locked automatically once main door operation is finished	

Table 2: Main Door Lock/Unlock

Mode of Operation	Fingerprint Scanner Mode	Voice Recognition Security Mode
Main Door Lock/Unlock	**Verified**	Not used
	Not used	**Verified**

5.1. Primary Door Unlock with RFID

As shown in the Figure 5, When a corresponding RFID tag is placed on to the RFID reader module it verifies its authentication and allow to unlock the primary door.

5.2. Primary Door Unlock with Bluetooth HC05

Bluetooth HC05 with its mobiles App paired system is as shown in the Figure 6, which is another security mode option for accessing primary door with its successful authentication.

Figure 6: Bluetooth Android Mobile Application

5.3. Main Door Lock/Unlock with Fingerprint Scanner

As shown in the Figure 7, the fingerprint scanner is one of the secondary stage security modules, which can lock or unlock the main door when it gets a proper authorization.

Figure 5:RFID Reader and Its Tag

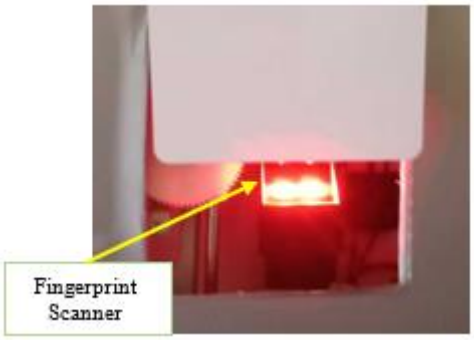


Figure 7: Fingerprint Scanner Module

5.4. Main Door Lock/Unlock with Voice Recognition Mode

As shown in the Figure 8, the voice recognition module can lock or unlock the main door by a valid authorization of its user.

Figure 8: Voice Recognition Module

5.5. Hardware Result of Primary Door Unlock

Primary door is a sliding door, which is unlocked by its commands of primary stage security system and the experimental result is as shown in the Figure 10. However, it is automatically locked with some time delay after every completion of secondary stage operation.

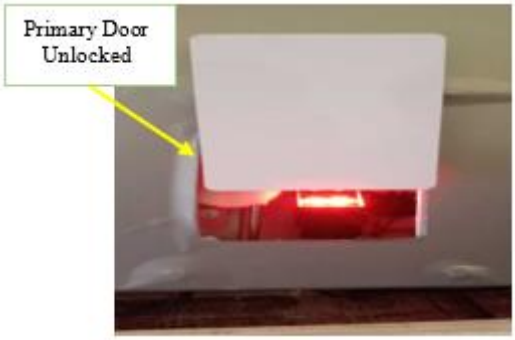


Figure 9:Hardware Result of Primary Door Unlocked

5.5. Hardware Result of Main Door Lock

As shown in the Figure 10, the main door operation is an internal locking mechanism by electromechanical device of linear actuator motor shaft, which will be hooked into the shaft holder by forward motoring action and then the holder keeps the shaft until the motor makes reverse motoring action.

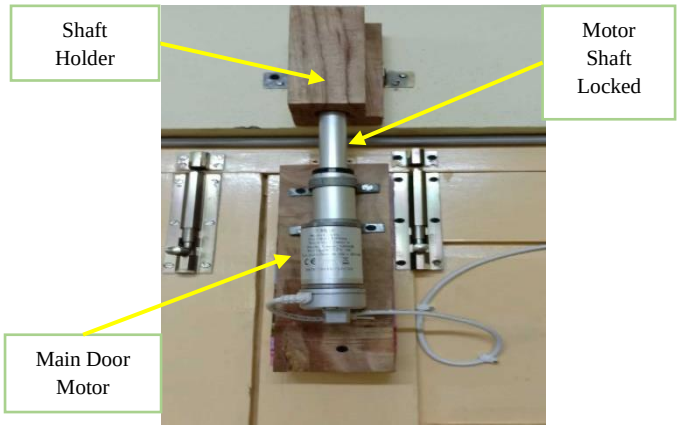


Figure 10: Hardware Result of Main Door Locked

5.6. Hardware Result of Main Door Unlock

The hardware result of main door unlock is as shown in the Figure 12, and is unlocked when motor shaft moves downwards (reverse motoring action) from the shaft holder by the commands of controller unit.

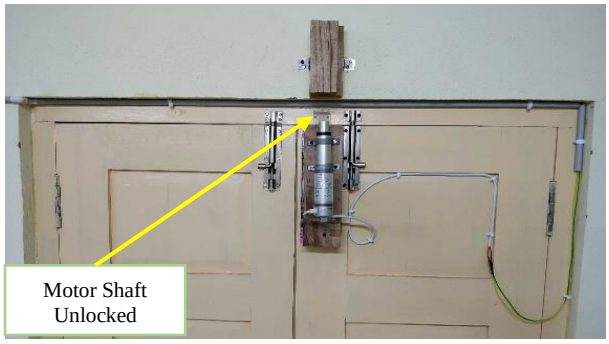


Figure 11: Hardware Result of Main Door Unlocked

5.7. LCD Display Unit Results

To understand the status of the operation, we provided a display unit which shows the step-by-step instructions to the user, then he knows whether the procedure is right or wrong.

Figure 12:LCD Display Alert

As shown in the Figure 13, the display unit directs us to unlock primary door by verifying a valid primary security key.

Figure 13:Display Result When No Primary Key Found

Not Found message will visible as shown in the Figure14 when no proper primary security key is matched.

Figure 14: Display Result When Authentication Success

As shown in the Figure 15, the success message tells that the primary stage security authentication is successful.

Figure 15: Display Result When No Proper Secondary Key Found

As shown in the Figure 16, Access does not grant message is used for authorization verification, when any one of its secondary stage securities is failed.

Figure 16: Display Result When Authorization Not Matched

As shown in the Figure 17, when no proper authorization is found, the system asks to check your credentials one more time.

Figure 17: Display Result When Authorization Matched

As shown in the Figure 18, The system is satisfactory about user's authorization and it permits to access the main door, however the primary door is automatically locked once main door operation is finished

Conclusion

In this paper, we present a novel smart lock device with an exceptional feature of internal and external security stages, which limits unauthorized access at its internal or at its external stage. Hence, whoever wants to access the system must pass his credentials at both security stages, then only the device allows user to access the door. Here the proposed solution uses complete wired communication between its controller unit and security modules, thus are non-internet connectivity (network) based, non-database required, non-OTP based systems. Therefore, the use of device is simple in operation and can be useful for any location (whether located area or remote location), easy understandable to any age factor people, faster in performance, efficient, trustful, and cheaper in cost.

References

[1] D.K.P. Gudavalli, I.S. Monica, M.E.C. Vidya Sagar, "A Novel Door Lock Operation Using Two Staged Smart Security Verification," in 2019 Global Conference for Advancement in Technology, GCAT 2019, Institute of Electrical and Electronics Engineers Inc., 2019, doi:10.1109/GCAT47503.2019.8978287.

[2] J. Pacheco, K. Miranda, "Design of a low-cost NFC door lock for a smart home system," in IEMTRONICS 2020 - International IOT, Electronics and Mechatronics Conference, Proceedings, Institute of Electrical and Electronics Engineers Inc., 2020, doi:10.1109/IEMTRONICS51293.2020.9216409.

[3] P.L. Teh, H.C. Ling, S.N. Cheong, "NFC smartphone based access control system using information hiding," in 2013 IEEE Conference on Open Systems, ICOS 2013, IEEE Computer Society: 13–17, 2013, doi:10.1109/ICOS.2013.6735039.

[4] R. Khalimov, Z. Rakhimbayeva, A. Shokayev, B. Kamalov, M.H. Ali, "Development of Intelligent Door Locking System Based on Face Recognition Technology," in ICMAE 2020 - 2020 11th International Conference on Mechanical and Aerospace Engineering, Institute of Electrical and Electronics Engineers Inc.: 244–248, 2020, doi:10.1109/ICMAE50897.2020.9178866.

[5] K.S.S. Javvaji, U.R. Nelakuditi, B.P. Dadi, "IoT Based Cost Effective Home Automation and Security System," in 2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020, Institute of Electrical and Electronics Engineers Inc., 2020, doi:10.1109/ICCCNT49239.2020.9225557.

[6] M. Shanthini, G. Vidya, R. Arun, "IoT enhanced smart door locking system," in Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020, Institute of Electrical and Electronics Engineers Inc.: 92–96, 2020, doi:10.1109/ICSSIT48917.2020.9214288.

[7] M. Pavelic, Z. Loncaric, M. Vukovic, M. Kusek, "Internet of Things Cyber Security: Smart Door Lock System," in Proceedings of International Conference on Smart Systems and Technologies 2018, SST 2018, Institute of Electrical and Electronics Engineers Inc.: 227–232, 2018, doi:10.1109/SST.2018.8564647.

[8] M.S. Hadis, E. Palantei, A.A. Ilham, A. Hendra, "Design of smart lock system for doors with special features using bluetooth technology," in 2018 International Conference on Information and Communications Technology (ICOIACT), IEEE: 396–400, 2018, doi:10.1109/ICOIACT.2018.8350767.

[9] S. Kavde, R. Kavde, S. Bodare, G. Bhagat, "Smart digital door lock system using Bluetooth technology," in 2017 International Conference on Information Communication and Embedded Systems, ICICES 2017, Institute of Electrical and Electronics Engineers Inc., 2017, doi:10.1109/ICICES.2017.8070788.

[10] V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga, S. Bojewar, "Intelligent security lock," in Proceedings - International Conference on Trends in Electronics and Informatics, ICEI 2017, Institute of Electrical and Electronics Engineers Inc.: 713–714, 2018, doi:10.1109/ICOEI.2017.8300795.

[11] M. Mathew, R.S. DIvya, "Super secure door lock system for critical zones," in 2017 International Conference on Networks and Advances in Computational Technologies, NetACT 2017, Institute of Electrical and Electronics Engineers Inc.: 242–245, 2017, doi:10.1109/NETACT.2017.8076773.

[12] M.K. Shafin, K.L. Kabir, N. Hasan, I.J. Mouri, S.T. Islam, L. Ansari, M.M. Karim, M.A. Hossain, "Development of an RFID based access control system in the context of Bangladesh," in ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems, Institute of Electrical and Electronics Engineers Inc., 2015, doi:10.1109/ICIIECS.2015.7193024.

[13] A. Kassem, S. El Murr, G. Jamous, E. Saad, M. Geagea, "A smart lock system using Wi-Fi security," in 2016 3rd International Conference on Advances in Computational Tools for Engineering Applications, ACTEA 2016, Institute of Electrical and Electronics Engineers Inc.: 222–225, 2016, doi:10.1109/ACTEA.2016.7560143.

[14] I.K. Hwang, J.W. Baek, "Wireless access monitoring and control system based on digital door lock," IEEE Transactions on Consumer Electronics, **53**(4), 1724–1730, 2007, doi:10.1109/TCE.2007.4429276.

[15] Y.T. Park, P. Sthapit, J.-Y. Pyun, "Smart digital door lock for the home automation," in TENCON 2009 - 2009 IEEE Region 10 Conference, IEEE: 1–6, 2009, doi:10.1109/TENCON.2009.5396038.

[16] A. Ibrahim, A. Paravath, P.K. Aswin, S.M. Iqbal, S.U. Abdulla, "GSM based digital door lock security system," in Proceedings of 2015 IEEE International Conference on Power, Instrumentation, Control and Computing, PICC 2015, Institute of Electrical and Electronics Engineers Inc., 2016, doi:10.1109/PICC.2015.7455796.

[17] S. Shavi, "Secured room access module," in Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017, Institute of Electrical and Electronics Engineers Inc.: 1134–1138, 2018, doi:10.1109/SmartTechCon.2017.8358546.
[18] M.T. Tombeng, R. Najoan, N. Karel, "Smart Car: Digital Controlling System Using Android Smartwatch Voice Recognition," in 2018 6th International Conference on Cyber and IT Service Management, CITSM 2018, Institute of Electrical and Electronics Engineers Inc., 2019, doi:10.1109/CITSM.2018.8674359.
[19] https://store.arduino.cc/usa/arduino-uno-rev3
[20] https://electronicshobbyists.com/rfid-basics-and-rfid-module-interfacing-with-arduino/
[21] https://components101.com/wireless/hc-05-bluetooth-module
[22] https://create.arduino.cc/projecthub/amalmathewtech/secure-your-logins-with-biometrics-30e7c3?ref=search&ref_id=r305%20finger%20print&offset=0