© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJIE

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/ijie
ISSN : 2229-838X e-ISSN : 2600-7916

The International Journal of Integrated Engineering

# Development of a Lock Biometric Authentication System for a Battery Powered Locking Device

**Iman Fitri Ismail[1*], Mas Fawzi[1], Wan Akashah Wan Jamaludin[1], Rais Hanizam Madon[1], Ahmad Fauzan Abdullah[2], Mohamad Ashik Abdullah[2]**

[1]Centre for Energy and Industrial Environment Studies (CEIES), Faculty of Mechanical and Manufacturing Engineering,
Universiti Tun Hussein Onn Malaysia, 86400, Parit Raja, Batu Pahat, Johor, MALAYSIA

[2]PT Reach International (M) Sdn Bhd,
Pearl Avenue, Jalan Pasir Emas, Sg. Chua, 43000 Kajang Selangor Darul Ehsan, MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/ijie.2021.13.02.003
Received 9 June 2020; Accepted 1 December 2020; Available online 28 February 2021

**Abstract:** This paper describes the development of a biometric authentication system in a battery-powered locking device. It differs from the conventional locking system, which connected to an external power supply. The system focuses on a fingerprint-based identification with single button operation. A fingerprint sensor readily available in the market was integrated with an Arduino as the processing unit to unify the button operation as means to trigger functions on the fingerprint sensor and actuator motors, as well as indicating lights for user feedback. The aim of the seamless fingerprint authentication requires a brief matching of users' fingerprints. A prototype of the system was built and tested. It was found that the device is able to match a fingerprint in less than 1s for up to 50 registered fingerprints. Using a nominal battery capacity of the 12V lithium battery pack with 5000mAh, the amount of current supply to the actuator is sufficient for 400 activations.

**Keywords:** Fingerprint sensor, Arduino, Internet of Things (IoT), Mobile security, One-key system

## 1. Introduction

The implementation of the Internet of Things (IoT) in daily application renders it necessary to be incorporated into a safety mechanism for the security of belongings [8]. IoT continues to revamp how personal and organizational security can be enhanced, especially since the application gives full liberty and access to the end-users on how he interacts with the system [10]. The smart lock that integrates IoT with a lock-based system offers remote connectivity to its user to allow for more flexibility on the system-user interaction and provides more security with real-time monitoring. It is one of the essential components for greater control of the home and personal security, providing privileges for visitors and family members to access the house via monitored secured access within the lock and the working of the device depends on remote activation via other devices such as smartphones [12]. Previous implementation and researches on the Internet of Things (IoT) for security purposes were integrated into house automation and security system. This includes the use of smart wireless set sensors connected together to detect access and intrusion into houses, but it is only limited to the use of infra-red (IR) and Bluetooth remote control integrated with smartphones for the users to gain access into the house [1].

Incorporating IoT into the traditional locks that have been the final defense line for centuries include the enhancement of the security that it can provide. The problem that persisted with traditional lock is the risk of the key being duplicated - since making a copy of the key is an easy task [9]. The progress of technology brought forward with

*Corresponding author: ifitri.ismail@gmail.com

the increasing complexity of locks, such as the use of Radio Frequency Identification (RFID) and the use of digital locks in hotels in the form of electronic cards that can be replaced and allow activation and deactivation based to give access to different tenants. The use of RFID is inexpensive, and it provides better control of access compared to the traditional locking system [11]. It also provides records of the user access via an onboard database system that needs to be configured by the owner which can be further expanded to include real-time monitoring over the internet [2].

A fingerprint module can limit access to users whose fingerprints are stored in the memory. Considering the fingerprints are stored within the module, fingerprints that are stored will retain themselves even after a power failure or the battery connected to the system is completely drained [3]. Hence, it provides a solution to the conventional problems that came with a traditional lock, such as the loss of keys.

The use of Radio Frequency Identification (RFID) is susceptible to different means of security attacks. Firstly, the computing capability and level of security protection depend on the cost of the RFID tag. The open radio signal of the communication link makes it convenient for the intrusion. The RFID tag can also be hacked to monitor the system behavior remotely, and the RFID cards can be duplicated which allows criminals to gain access through the RFID based locking system [4]. The addressed concerns along with the advantages and conveniences provided by the fingerprint locking system, making it necessary for this method of access to be studied.

The integration of this smart locking system will provide records when the system is accessed or tampered with so that the homeowners can keep track and give entry to visitors, for example, via registration and removal of fingerprints. The fingerprints accesses will be recorded for the system owner to monitor the in and out movements of the registered fingerprints within the house in which the device is fitted. The device can also be integrated with the current over the internet lodging services such as Airbnb and homestays. The use of battery-operated locking devices has several advantages and has its niche application in the security of valuable belongings. This paper contains the development of a lock biometric authentication system for a battery-powered locking device.

## 2. Selection of Hardware

Prototyping phase utilizes variants of Arduino prototyping boards; they were tested based on their ability to receive inputs and execute processing based on users' predetermined input of the C language on the integrated circuit of the board via Arduino Integrated Development Environment (IDE). Arduino boards are inexpensive compared to other prototyping methods, and it provides a clean and concise environment for prototyping. The open-source nature of the boards allows for the prototype to be further refined and developed according to the schematics and unclassified components of the board. It is cheaper compared to other microcontrollers in the market. The Arduino Integrated Development Environment (IDE) also enhances the understanding and interactions with the board. It is also open source, allowing for future research and commercialization of the developed system [5]. For this project, an Arduino Mega 2560 was selected as the medium of prototyping since it consists of 54 digital input and output pins. It comes with 16 analog inputs and 4 hardware serial ports or UARTs. Thus, any peripheral and components connection can be directly routed to the board instead of utilizing extra external modules which will incur more cost and space. Fig. 1 shows the schematic of an Arduino Mega 2560 prototyping board including the explanation of digital and analog pins.

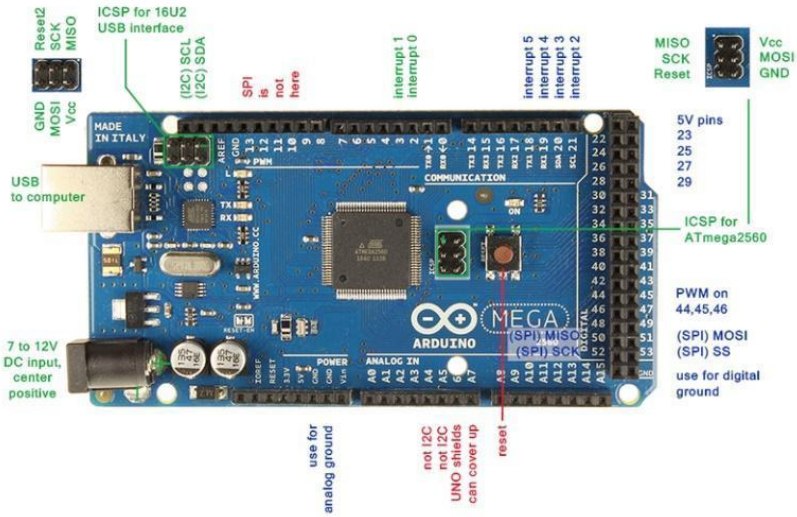



**Fig. 1 - Arduino Mega 2560**

The design of this lock uses a capacitive sensor that reads the image from the user's thumb and granting access only to a pre-registered fingerprint. Hence, the fingerprint module will act as the main input within the embedded locking system. R300 UART Interface Capacitive Fingerprint was used as a fingerprint reader. The fingerprint image

and the user data storage are encrypted collectively on the onboard chip. R300 can adapt to different conditions of the fingers during the reading process, such as charred or wet fingers due to its high recognition rate. It requires a low voltage of 4.0 V for a 508 DPI fingerprint resolution. The verification and scanning speed are less than 0.3 seconds. The locking system is expected to work even in high humidity. Thus, the R300 fingerprint reader can withstand working humidity up to 85%. [6].

**Fig. 2 - R300 UART Fingerprint Reader**

## 3. Proposed Solution

A proposal made to address the problems in the form of a lock that incorporates both mechanical and electrical operation into its operation, Figure 3; hence making the lock an electromechanical device. Opting the use of a fingerprint sensor as a means to replace the mechanical based lock. The sensor eliminates the issues of lost keys and jammed locks. The inspiration for a simpler architecture of an electronic system with small power consumption is to sustain the lifespan and operational hours of the locking device. The lock adheres to the working principles of the conventional locking device, in which the authentication procedure and access are given directly from the microcontroller to minimize remote tampering and foreign intrusion [7]. The functionality of the system can be enhanced further, provided that bigger battery capacity is available to sustain or extend the operational hours of the locking device.

Since the lock is electronic based, it also improves the security by making it more resistant to tamper and breaking of locks as it is meant to deter potential or unwanted access at first glance. The feature also serves to protect the mechanical components from tamper by having it on the internal compartments, away from external access. Partnered with a single button operation and an LED indicator offers a simple yet robust piece of equipment. The single button operation input is fed into a processor that links it to certain features based on its input, such as registering a user, deleting the user, and authenticating the user. It is used to trigger one of the operations, and the LED provides feedback to the user via its operation state.

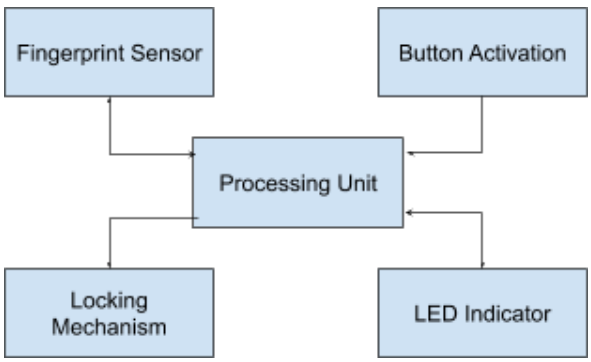



**Fig. 3 - Interactions of components in the lock system**

## 3.1 Functions and Features

Per mentioned in the previous point, the function of the button was enhanced with the ability to provide multiple inputs trigger various features available with the fingerprint sensor.

i) Reset user
ii) Authenticating user

The reset user feature allows the owner to delete an existing user and register a new user to the device; the authentication feature will prompt the user for input on the sensor to identify the registered user which is followed by the actuation of the internal actuator to unlock the lock. The process of deleting, registering or adding and authenticating users follows the set of a flow process that begins at the activation of the locking system via a button.

## 3.2 Process Flowchart

The interaction of the lock utilizes the two functions in the fingerprint sensor as highlighted in Fig 4. The process flow will be triggered upon a user interaction at the button; then it will identify the single button command for unlocking the unit; else, it will prompt a reset function on the lock.

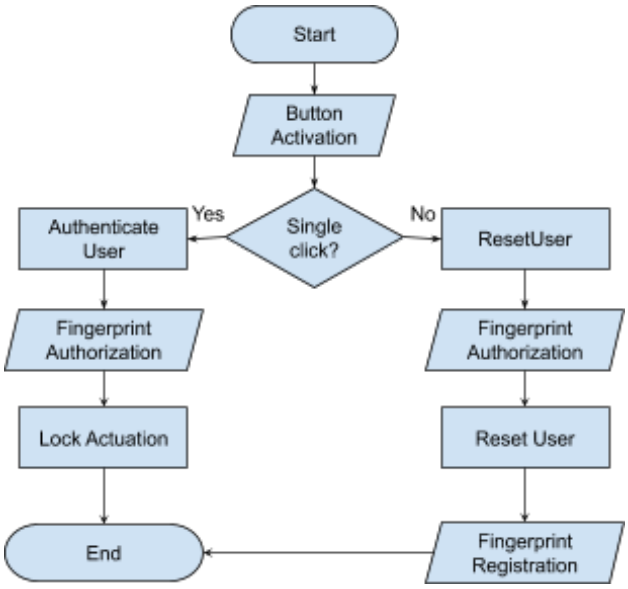



**Fig. 4 - Process flowchart of lock functions**

In the authentication process, the fingerprint of users was scanned on the fingerprint module, and the programming algorithm will compare the entered fingerprints with the available images within the database. If the image of the fingerprint matches the entered fingerprints, the motor in the lock will be actuated as the final response of the device. The locking mechanism must be engaged manually by the user to set it in a locked state.

The reset function will only be accessible if the owner of the fingerprint that the lock is bound to authorize a reset cycle, hence deleting the owner bind and awaits a new owner to register as the new fingerprint bind is made. Upon double-clicking the button, the device will enter authorization mode that allows for the fingerprint to be scanned and entered as an image. The authorization mode ends once the fingerprint is scanned on the module and the user can authenticate the fingerprint by pushing the button with a single click.

## 3.3 Wiring Structure

The core of the unit is the Arduino Mega 2560, all the interaction for both power and signals are connected to the unit as illustrated in Fig 5. The figure is split into four categories designated by color, red, blue, green and orange. The red region borders the power circuit, receiving power from a USB connection to a charging circuit before passing it to the battery for charging. The battery is also equipped with a voltage regulator ensuring a steady voltage supply to the Arduino. Indicated in blue is the Arduino Mega as the brain of operation taking power from the latter connecting it to the fingerprint sensor in green. In orange host the input and output interaction available in the lock, the one-button switch, the lock motor, and the fingerprint reader.

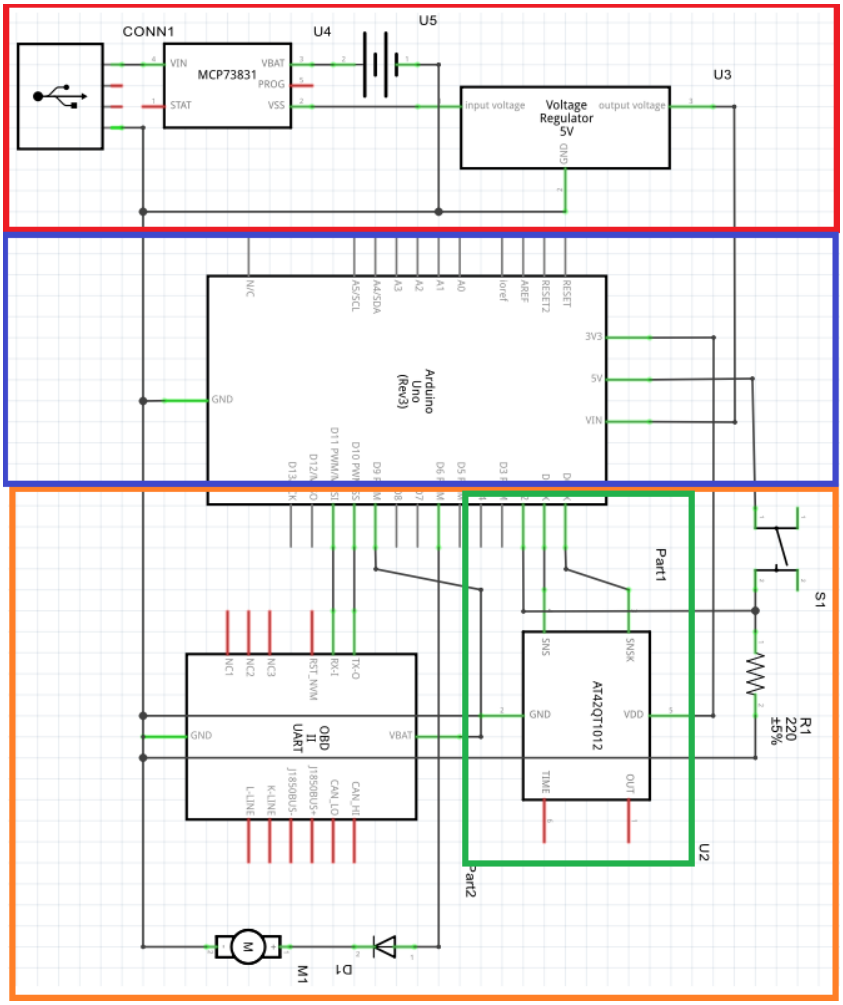



**Fig. 5 - Schematic diagram on wirings of the lock unit**

## 3.4 Power Consumption

The calculation of power consumed by the system requires the determination of supply voltage and current. Table 1 is the technical specification of Arduino Mega, an aspect of the operation that was considered in studying the power consumption of the locking system.

**Table 1 - Technical Specifications of Arduino Mega ATmega2560**

| Parameters | Value |
|---|---|
| Operating Voltage | 5V |
| Recommended Input Voltage | 7-12V |
| DC Current per I/O Pin | 20 mA |
| DC Current for 3.3V Pin | 50 mA |

The operational time for the locking system when it is activated is 5 seconds. Hence, the operational power consumption for the active session varies when compared with the passive session. The power consumed by the following components: R300 fingerprint sensor, LED light, motor culminated into the total active power consumption during the 5 seconds activation. Table 2 below shows the overview of battery information.

**Table 2 - Power Supply Specification**

| Parameters | Values |
|---|---|
| Nominal Voltage | 11.1V |
| Output Voltage | 8V – 12.6V |
| Nominal Capacity | 5Ah |
| Nominal Power | 60Wh |
| Life Cycle of charging | 500 times |

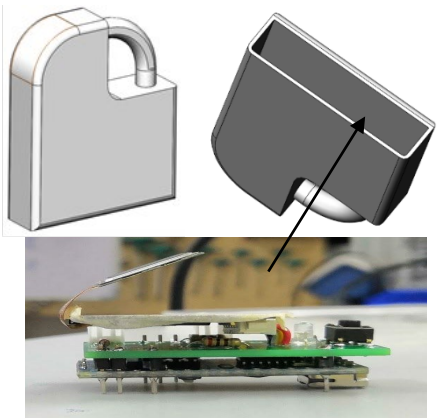
Hence, with average activation of the system 10 times daily, it is expected that the locking system can sustain itself with a full charge of around 3 months. The system will sustain to work longer hours in an inactive state, where the state of the microprocessor is idle. The connection with the button still maintains a low level of activity for it to receive input and activated based on an interrupt trigger; this state of activation is the most critical to extending the lifetime of the battery. The locking system requires 90 minutes of charging based on the specification of the 12V 5000 mAh Lithium battery pack.

## 3.5 Fingerprint Module

The process of retrieving the fingerprint includes the enrollment and matching of fingerprints. The enrollment of the fingerprint will generate the template and store it in the on-board chips. Thus, when the fingerprint authentication is performed, the fingerprint entered will be compared with the templates in the library. The module communicates with the microprocessor via UART and can store up to 150 fingerprints. The fingerprint module is efficient at a working temperature of $10℃$ to $60℃$ with relative humidity below 80%. It is selected due to the discrete size that allows it to be fitted inside a confined form factor and is also able to support $360°$ of fingerprint recognition by increasing the intelligent repair processing of incomplete fingerprint images.

**Table 3 - Technical Parameters of R300**

| | |
|---|---|
| Fingerprint Extraction time | 0.45 seconds |
| Fingerprint Matching time | 0.45 seconds |
| Capacity | 150 fingerprints |
| Operating Voltage | 3V |



Electronic part section

**Fig. 6 - Final prototype form factor**

## 3.6 Prototype

A prototype was built to test the functions and features, as well as optimizing the circuit design and form factor. Noted in Fig.6 is the fourth iteration prototype made to finalize the project includes a small form factor of only 2 cm in thickness. It shows the circuitry that connects all the components used in the project into a single compact PCB hence enabling the project to achieve a small form factor. The form factor shall be inserted into a mechanical lock which is designed to be portable, which includes a power pack unit consisting of a battery and USB charging unit.

## 4. Results and Discussion

The development of the integrated locking system utilizes the use of electronic fingerprint recognition as its core component. This integration will provide the users with keyless entry, and high accuracy of individual identification as the biometric relies on the physical traits that are arbitrary to each respective individual. The device will not unlock if the accessing users' fingerprint IDs are not registered within the microprocessor, and this will discourage the event of false entry that comes with less safe conventional locks due to stolen or duplicated keys. Any attempt using unregistered fingerprints will activate a blue LED.

The use of the fingerprint module will not abide by the predetermined response time as stated in the technical parameters as the database becomes more crowded with an increasing number of registered fingerprints. Therefore, evaluation of the performance of the fingerprint verification system was conducted by studying the time taken for fingerprint matching against the increasing number of registered users. Fig. 7(a) shows the response of fingerprint matching time measured in seconds against the total registered fingerprints that are stored within the database.

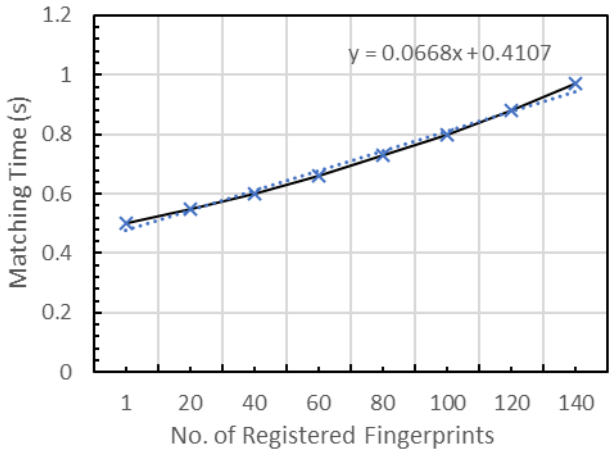



**Fig. 7 - Fingerprint matching time**

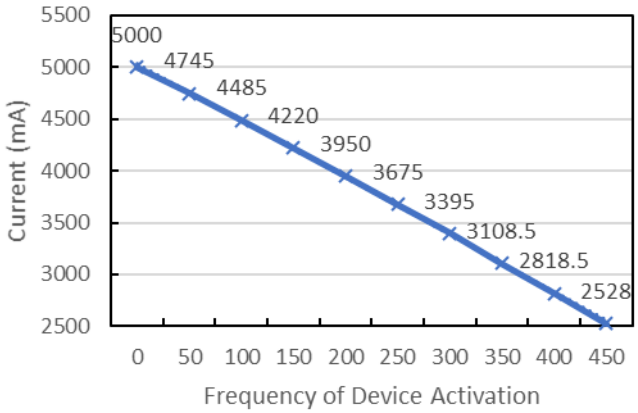



**Fig. 8 - Battery life cycle per full charge**

There is an increase in time taken for the fingerprints to be matched with the images in the database due to the capability of the fingerprint module. This limitation exists due to the organization of codes and the capability of the fingerprint module in making comparison of entered fingerprints with the registered fingerprint images. As the number of stored fingerprints increases, the time taken for it to be matched increases. The structure of the programming algorithm is detrimental in ensuring that every process in authentication is carried out as brief as possible. The matching time does not exceed 1s for up to 140 registered fingerprints. The matching time for any number of registered fingerprints adheres to the linear relationship of $y = 0.0668x + 0.4107$ with the minimum of one fingerprint and maximum of 150 registered fingerprints.

The nominal battery capacity of the 12V Lithium Battery Pack is 5Ah, or equivalent to 5000mAh. Discharge characteristics were examined to determine the optimum operational activation of the device during user interaction. Thus, the maximum number of activations before the battery is discharged can be determined. Theoretically, the

connection of the fingerprint modules, push buttons and the actuators will draw 70mA. The consumption rate of the battery is 0.7, and the estimated battery life per full charge is 50 hours. The capacity of the battery is calculated based on the following formula.

$$Battery\ Life = \frac{Battery\ Capacity\ (mAh)}{Load\ Current\ (mA)} \times 0.7$$

The factor of 0.7 mA accounts for the allowable external factors that affect the longevity of battery life. Based on the experimental analysis on the device activation against the available electric charge measured in Ampere-hour (Ah), it can be observed that the battery life is adequate up to 900 activations which tallies with the approximation given by the trendline equation $y = -274.95x + 5304.7$ in which 450 activations consumed half of the charge on the battery.

## 5. Conclusion

The application of the Internet of Things (IoT) had been the subject of various studies especially on the use of biometrics to enhance the security of its users via the integration of mechanical and electrical aspects. In this research, fingerprint identification has been implemented in a battery-operated locking system, incorporated with the process of user authentication and user ID verification. The system provides a keyless entry method that discourages methods of forced entry such as via duplicated or stolen keys. The owner of the device can add and remove users at any time, with the interaction of each registered user recorded with the devices will be sorted according to time of access; making it a more preferred choice compared to the normal entry via keys. The system can be placed in an enclosure and implemented for the use of housing, vehicles or any commercial building security.

## Acknowledgement

This study is part of collaborative research and development between Universiti Tun Hussein Onn Malaysia and PT Reach (M) Sdn Bhd under a matching grant vot. A148 and H003.

## References

[1] Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016). IoT based smart security and home automation system. 2016 International Conference on Computing, Communication and Automation (ICCCA). doi: 10.1109/ccaa.2016.7813916

[2] Verma, G. K., & Tripathi, P. (2010). A Digital Security System with Door Lock System Using RFID Technology. International Journal of Computer Applications, 5(11), 6–8. doi: 10.5120/957-1334

[3] Kawale, A. (2013). Fingerprint based locking system. International Journal of Scientific & Engineering Research, 4(5).

[4] Wang, Q., Xiong, X., Tian, W., & He, L. (2011). Low-Cost RFID: Security Problems and Solutions. 2011 International Conference on Management and Service Science. doi: 10.1109/icmss.2011.5998331

[5] Nayyar, A. (2016). An Encyclopedia Coverage of Compiler's, Programmer's & Simulator's for 8051, PIC, AVR, ARM, Arduino Embedded Technologies. International Journal of Reconfigurable and Embedded Systems (IJRES), 5(1), 18. doi: 10.11591/ijres.v5.i1.pp18-42

[6] Afolab, A. O., & Alice, O. (2014). On Securing a Door with Fingerprint Biometric Technique. Transactions on Machine Learning and Artificial Intelligence, 2(2), 86–96. doi: 10.14738/tmlai.22.164

[7] Ping, W., Guichu, W., Wenbin, X., Jianguo, L., & Peng, L. (2010). Remote Monitoring Intelligent System Based on Fingerprint Door Lock. 2010 International Conference on Intelligent Computation Technology and Automation. doi: 10.1109/icicta.2010.436

[8] E. Knight, S. Lord and B. Arief, "Lock Picking in the Era of Internet of Things," *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, 2019, pp. 835-842. doi: 10.1109/TrustCom/BigDataSE.2019.00121

[9] Y. Nagaratnam and W. K. Wong, "Miniature Digital Pin-Number Lock," *2010 Second International Conference on Computer Research and Development*, Kuala Lumpur, 2010, pp. 686-691. doi: 10.1109/ICCRD.2010.158

[10] M. T. Tombeng and H. S. Laluyan, "Prototype of authentication system of motorcycle using RFID implants," *2017 5th International Conference on Cyber and IT Service Management (CITSM)*, Denpasar, 2017, pp. 1-5. doi: 10.1109/CITSM.2017.8089235

[11] Nadia Nedjah, Rafael S. Wyant, Luiza M. Mourelle, Brij B. Gupta, Efficient fingerprint matching on smart cards for high security and privacy in smart systems, Information Sciences, Volume 479, 2019, Pages 622-639, doi: 10.1016/j.ins.2017.12.038

[12] Pavel Blazek, Ondrej Krejcar, Daniel Jun, Kamil Kuca, Device Security Implementation Model based on Internet of Things for a Laboratory Environment, IFAC-PapersOnLine, Volume 49, Issue 25, 2016, Pages 419-424, doi: 10.1016/j.ifacol.2016.12.086