

Fingerprint Based on Medical Information & Patient Retrieval

Rufiney Kalaiselvan¹, Azlina Bahari^{1*}

¹ Department of Electrical Engineering Technology, Faculty of Engineering Technology,
Universiti Tun Hussein Onn Malaysia, 84600 Pagoh, Johor, MALAYSIA

* Corresponding Author Designation

DOI: <https://doi.org/10.30880/peat.2021.02.02.057>

Received 13 January 2021; Accepted 01 March 2021; Available online 02 December 2021

Abstract: The emergence of electronic health or eHealth systems has revolutionized the healthcare industry to offer better healthcare services at a low and affordable cost, but it still suffers from security and privacy issues in handling health information. The privacy and security issues in the eHealth domain are mainly centered around user authentication, data integrity, data confidentiality, and patient privacy protection. Therefore, biometrics technology has considerable opportunities to cope with the above security problems by providing reliable and secure user authentication. The major aim of this study is to design and implement a Medical Management System with fingerprint biometrics for authentication. The core functionalities of this system were designed using Microsoft Visual Basic.Net. The client application provides access to patient records implemented with Microsoft Access. However, due to the sensitive nature of health data, the most important challenge lies toward the development of an efficient security model that can guarantee data privacy and reliability, verifying that only authorized personnel can access their corresponding health data. A two factors authentication which includes pin and biometrics was used to ensure the security and protection of the system. In this study, a comprehensive overview of biometrics applications in e-health has been conducted.

Keywords: e-Health Systems, Biometric Technology, Authentication System

1. Introduction

Medical information is the most sensitive and important information in terms of privacy which implies all information related to the patient. A robust and effective medical information system should be made up of storing, editable, and making available all clinical information to the doctors and staff for the patient care. The medical system should be linked to all the data based on interaction of the patients with the health structures, such as general practitioners, specialists, health institutes, hospitals and pharmacies [1]. By introducing the Biometrics fingerprint technology in the medical information system, the hospitals are committed in maintaining the patient's privacy while sharing data to improve the diagnosis and treatment of patients. Moreover, incomplete, or misunderstood healthcare records can

*Corresponding author: lina@uthm.edu.my

2021 UTHM Publisher. All right reserved

publisher.uthm.edu.my/periodicals/index.php/peat

lead to wrong medication that may eventually cause the death of a patient. Health Management Systems are built to eliminate the bulky paperwork in hospitals and to address the shortage of healthcare personnel [3]. Furthermore, Fingerprints have the potential to offer high security, friendly users, and more convenience for user authentication because fingerprints cannot be lost or forgotten like passwords and cards [4]. In addition, fingerprints are significantly more difficult to copy, share or even distribute than passwords. This is what makes fingerprint recognition the most convenient method while maintaining a sufficiently high security. The emergency data set of the patient such as blood type and contact person information can be accessed using the patient finger in the emergency medical situation [5].

The advantages of the fingerprint medical information system over other systems are:

- Consumptions of low power
- Increase security formats in the hospital
- Able to add and delete patient users
- Patient database maintained individually so that able to avoid the man-made error

The efficient use of the fingerprint based medical system is the easy, not complicated and fast data access facility which leads to implementation of particularly widespread security systems. Moreover, this system uses a secure and authenticated data communication between clients and database servers over distributed object protocol [6]. This system is developed on Microsoft Visual Basic 2010 platform by using an Object-oriented architecture and design patterns which allows physicians to make better and safer medical decisions for their patients. This may result in a higher quality of care and the avoidance of unnecessary invasive testing. Our long-term goal is to create a sustainable, secure solution and a user friendly system which allows doctors and staff to more efficiently utilise patient data to improve the overall quality and efficiency of health care [7]. Every day, millions of patients in Nigeria visit doctors in clinics and other health care providers however, these visits mostly introduce new medical records or builds on existing one, and therefore entails the retrieval of a particular patient record. The approach for storing and retrieving records requires the deployment of dependable technology with efficient users' authentication. Patients want to have assurance that the privacy of their records are well kept [8]. Consequently, a health management system with integrated fingerprint biometrics could provide some level of security for patients and healthcare professionals.

The specific aim of this study is to develop an e-health system with fingerprint biometrics and password or pin for authentication. The system developed is named as the Medical Management System. The remaining part of the paper is described as follows: section 2 explains in detail the literature review while section 3 contains materials and methods, section 4 provides the system implementation, and section 5 highlights the discussions and recommendations.

2. Literature Review

There are several Medical Management Systems that make use of passwords as authentication for patient records. Meanwhile, a lot more research on techniques for fingerprint biometrics are desirable in literature, particularly those that integrate more than one factor authentication scheme. Some of the biometrics-based Medical Management Systems are discussed in this section.

Lamport developed an authentication scheme using password for authenticating user access remotely [9]. Darrell explained in [10] how the implementation of biometrics is used in identifying security issues and increasing information security for doctors, nurses, and patients in healthcare industries. It also explores the contribution of biometrics in improving security measures within the healthcare industry for protection of all the entities which involved doctors, nurses and patients. [11] developed a smart-card system with password authentication scheme using biometrics technique and hash function. This system gave a secured and efficient Tele-care system.sector. The study showed a great opportunity for applying biometrics technology in e-Health for reliable security solutions.

Manimekalai [12] carried out a review on the different biometric techniques used in health care systems and proposed a new method for biometric health care systems for the unconscious state of humans. The authors noted that the health care system has entered the cloud and particularly took the problem of heart attack patients as a case study. [13] featured privacy policies to access a central health record database using biometric identification. The study was implemented real time and the results demonstrated an improved response time of 19.8 seconds with above 200,000 patients recorded in the system. [14] investigated and analyzed several Telemedicine, e-Health and Wellness (TEW) systems. The study concluded that most of the wireless sensor based TEW development systems focus on engineering issues. [15] applied bimodal (face and fingerprint) authentication measures to secure patient medical information within a system. [16] proposed a novel approach using mutual access and tri-factor authentication protocol for body sensor networks (BSN) in healthcare application. The paper concluded that the proposed protocol is better than existing bi-factor user authentication schemes. [17] proposed security solutions to secure communication between the patient, its device, and the network channel. Biometric technology using heart sounds is applied in the technology of authentication in Body Area Network Technology [18].

3. Materials and Methods

This section demonstrates the proposed user authentication scheme using fingerprint biometric to control access to an electronic healthcare system.

3.1 Materials

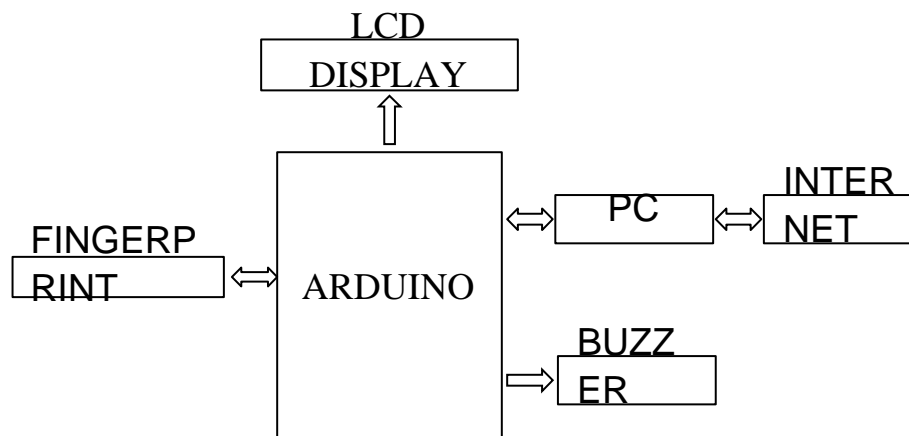


Figure 1: Block Diagram

Microsoft Visual Basic

- **The Administrator:** This module handles all the changes that are made in the database and the enrollment of users. Each user enrolled in this module is given privileges by selecting their status.
- **Registration:** This module handles the registration of patients in the reception or allocated office and, assignment of patients to available doctors.
- **The Doctor:** This module allows the doctor to give medications to patients, view the bill and history of the patient.
- **The Nurse:** This module allows the nurse to view and give medications given to patients and then give patients invoice.

Arduino Uno

The Arduino Integrated Development Environment or known as Arduino Software (IDE) contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus [19]. It connects to the Arduino and Genuino hardware to upload

programs and communicate with an integrated development environment (IDE) which is also known as integrated design environment or integrated debugging environment. This software is an application that provides comprehensive facilities to computer programmers for software development. An IDE normally consists of:

- A source code editor
- A compiler/or an interpreter
- Build automation tools
- A debugger

IDEs is a single program in which all development is done. This program provides many features for authoring, modifying, compiling, deploying and debugging software. The main aim is to abstract the configuration together with the command line which utilities in a cohesive unit. This reduces the time to learn a language and increases the developer productivity. It is also thought that the tight integration of development tasks can further increase productivity. For example, code can be compiled while being written, providing instant feedback on syntax errors [20].

- Fingerprint Sensor

A biometric fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image was called a live scan. This live scan was digitally processed to create a biometric template, collection of extracted features which was stored and used for matching of fingerprint. A fingerprint scanner system has two basic jobs which mainly it needs to get an image of the finger and secondly it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images [21].

- Electric Component
 - LCD Display
 - Led
 - Buzzer
 - Resistor

3.2 Methods

The flowchart in Figure 2 shows the process flow of user's registration, system access through consultation, drug administration and patient treatment. First, the patient has to register, and receptionist checks for the doctor's availability. Thereafter, patients consult the available doctor and room is allocated to the patient if recommended for admission. Continuous medication is given to patients and is discharged if certified healthy by a doctor.

A deployment diagram was also created with four objects namely Desktop client, Hospital Local Server, Printer and Database Server. The Desktop client serves as the user interface through which patients, doctors and administrators interacts with the system. The Hospital local server provides application services, the different modules that make up the software and also storage of medical data. The form in Figure 3 is used to authenticate administrators for access to enroll users into the system. The users are expected to place their right thumb finger on the fingerprint scanning machine. Improper placement of finger on the machine will report, please place the enrollment finger on the fingerprint scanner. The Class diagram comprises five objects which are Enroll, Patientinfo, Assigned, Inpatient and Treatment. A non-medical staff can register the patient. A non-medical staff and nurse go through the process of enrolment with the system. Each doctor also gets enrolled with the system. The nurse can give medication to the patient according to the system.

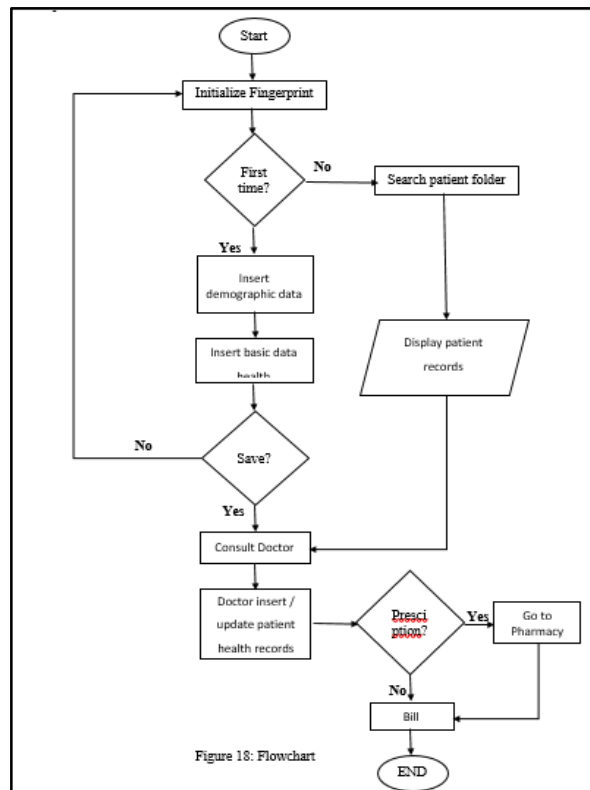


Figure 2: Flowchart of Medical Management System

4. Results and Discussion

This part will discuss the result of the project that has been tested to obtain the data of the Fingerprint scanner which includes enrollment. login page The developed prototype has been completed and its functionality has been fully tested which strives to achieve the objectives of this project. All the data obtained from the database has been presented in a table form.

4.1 Results

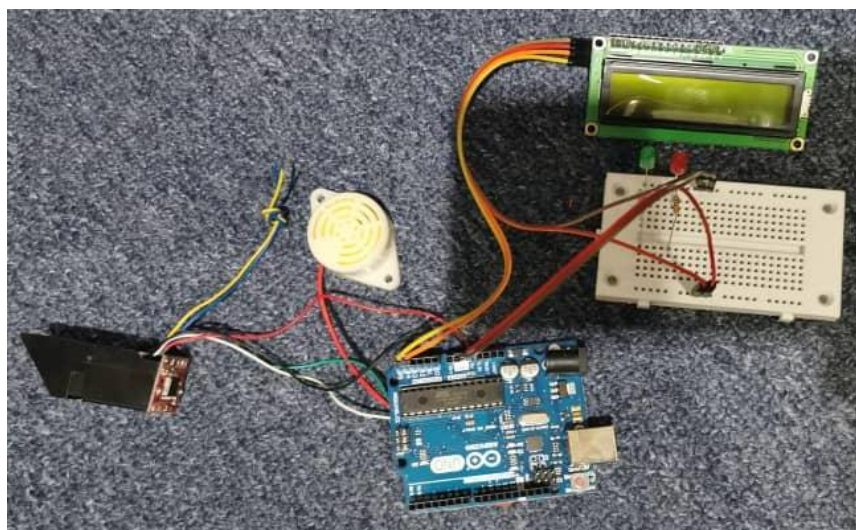


Figure 3: The connection of fingerprint scanner and arduino

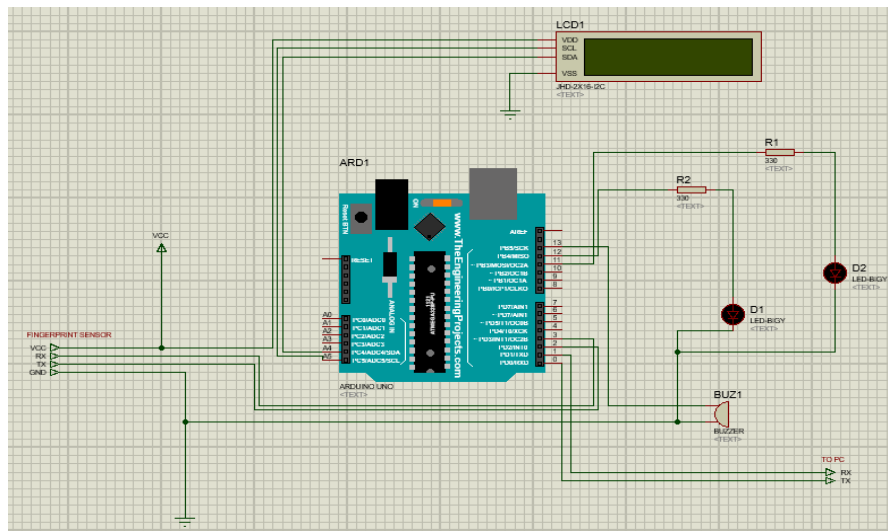


Figure 4: the schematic drawing of the Arduino system



Figure 5: home page of the Medical Management System



Figure 6: login page of the Medical Management System. The page contains username and password

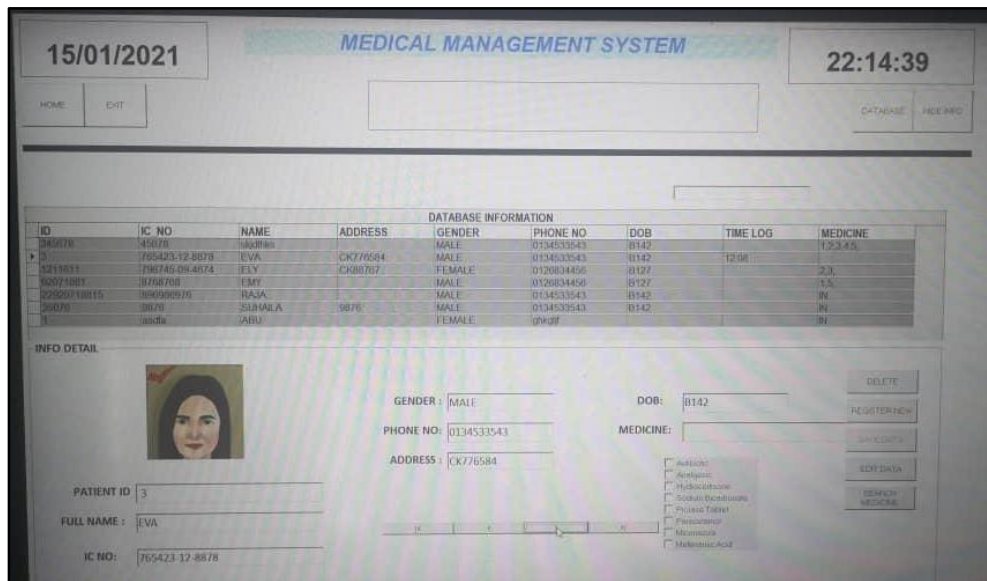


Figure 7: the database information which contains the patient id, Full name, address, phone number, date of birth, gender, marital status, occupation and blood group. The other data requested for patient registration includes surgical history details and allergies



Figure 8: shows the LCD display of the Medical Management System



Figure 9: process of the verification and storing of the patient fingerprint once the patient registered in the system

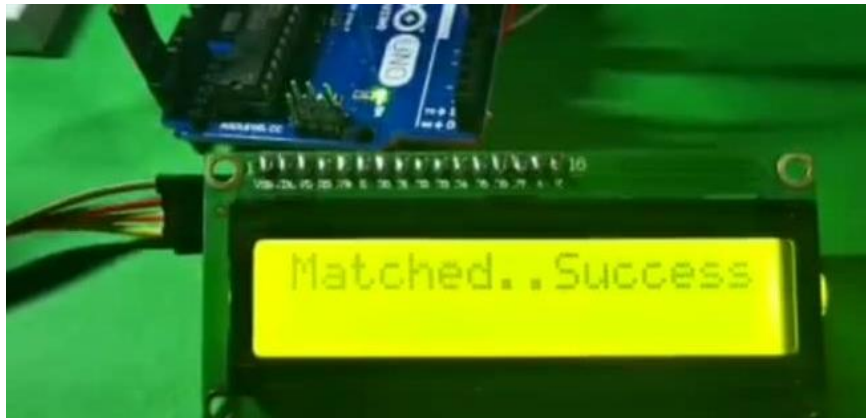


Figure 10: the results after verifying the patient’s fingerprint to ensure that the patient is who he/she claims to be

4.2 Discussions

Biometrics is making it possible for patients and healthcare professionals to feel secure that their information is being kept confidential and is only being released to those who have the right to see it. Advances in Biometrics technologies have formed an extensive array of secured authentication, verification and identification solutions. Fingerprint technology is one of the most popular biometrics technology used for authentication by several people globally because of its low cost and power consumption. The efficient use of the fingerprint-based e- medical system is the easy and fast data access facility leads to implementation particularly widespread in security systems. Moreover, the emergency data set such as his/her blood type and contact person information can be accessed using the patient's finger in the emergency medical situation when the patient is unconscious. Thus, the patient database is maintained individually so that we can avoid the man-made error. Furthermore, the fingerprints are significantly more difficult to copy, share, distribute than passwords which makes fingerprint recognition the most convenient method while maintaining sufficiently high security. Other than that, fingerprint-based e-medical system is the use of electronic methods for collecting, storing, processing, and accessing patient medical records that have been stored in a multimedia database management that records all data that is very personal and contains information about identity, examination, treatment, actions, data medical, demographic and every service in the management of patients in hospitals and clinics.

5. Conclusion

In my project, fingerprint verification is considered to protect the medical information transmitted and to guarantee both the integrity and the confidentiality of the data. Patient data can be stored and retrieved by connecting to the hospital database, and thus it can be accessed globally. The main advantage of this project is the online accessibility of the patient database. Another crucial advantage is that it is applicable during emergency conditions. The patient need not carry the ID card with them as such there is no possibility of losing them. Medical record errors can be reduced using the fingerprint technique. Since fingerprints cannot be lost or forgotten like passwords, fingerprints have the potential to offer high security and more convenience for user authentication. The fingerprints are significantly more difficult to copy, share, distribute than passwords which make fingerprint recognition the most convenient method while maintaining sufficiently high security. Furthermore, large fingerprint data need not be memorized. The emergency data such as his/her blood group and type and contact person information can be accessed during his/her finger in the emergency. Our long term goal is to create a sustainable, secure solution that allows doctors to more efficiently utilize patient data to improve the overall quality and efficiency of care. In future, the Patient database can be modified with images like

X-ray, CT, MRI and graphs such as ECG, EEG and EMG. In addition, we can upgrade the system by the patient gets a message upon their appointment date with the doctor.

Acknowledgement

The authors would like to thank the Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia for its support.

References

- [1] Zuowen T. "An efficient biometrics-based authentication scheme for telecare medicine information systems." *Przeegląd Elektrotechniczny*, 2013, pp. 200-204.
- [2] Andreeva, E. "Alternative biometric as method of information security of healthcare systems." *Proceeding of the 12th Conference of FRUCT Association Department of Information Security Technologies*, 2012, pp. 210-214.
- [3] Azeta, A. A., et al. "Preserving patient records with biometrics identification in e-Health systems Data." *Engineering and Applications*, 2019, pp. 181-191. https://link.springer.com/chapter/10.1007/978-981-13-6347-4_17, doi.org/10.1007/978-981-13-6347-4_17.
- [4] Bazin, A. "Biometrics for patient identification." *A US case study.*, 2012. "Biometric Identity in Healthcare: Reduces Health Care Fraud, Improves Patient Care and Protects Patient Privacy." <http://www.ibia.org/download/datasets/727/>, July 2011.
- [5] B. Spence. "Hospitals can finally put a finger on biometrics." <http://www.securityinfowatch.com/article/10473265/hospitals-can-finally-put-a-finger-on-biometrics>, 4 November 2011.
- [6] G. D. Mogli / Sri Lanka Journal of Bio-Medical Informatics 2011;2(4): 156-165 Atlas, Preserving Patient Records with Biometrics Identification in E-Health Systems
- [7] Diaz-palacios,, et al. "Biometric Access Control for e-Health Records in Pre-hospital Care." *EDBT/ICDT*, March 2013.
- [8] D.P. Mirembe. "Design of a secure framework for the implementation of telemedicine, eHealth, and wellness services." *Google Scholar*.
- [9] Esam, O. A, et al. "Biometric authentication system to protect sensitive medical data. Bimodal Biometrics for Health Care Infrastructure Security." *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, vol. Volume 1, March 2014.
- [10] Darrell S. "Implementing into the healthcare industry increases the security for the doctors, nurses, and patients." *Biometrics*, 2013.
- [11] Jhaveri H., and D. Sanghavi. "Biometric security system and its applications in healthcare." *International Journal of Technical Research and Applications*, 2014.

- [12] Manimekalai S. “Study on Biometric for Single Sign on Health Care Security.” *International Journal of Computer Science and Mobile Computing*, vol. Volume 3, no. Issue 6, June 2014, pp. 79-87.
- [13] Mason, Janelle, et al. “An Investigation of Biometric Authentication in the Healthcare Environment.” *Science direct*, vol. Volume 8, December 2020, pp. 1-10. (<http://www.sciencedirect.com/science/article/pii/S2590005620300278>), <https://doi.org/10.1016/j.array.2020.100042>.
- [14] Mesmoudi, S, and Feham, M. “biometric symmetric keys to secure wireless body sensors networks.” *Int. J. Netw. Secur. Appl. (IJNSA)* 3(5), 2011, pp. 155-166.
- [15] Schneider, and John K. “Positive Outcomes Implementing Biometrics in Multiple Healthcare Applications.” 2011. <http://www.ultrascan.com/Portals/16/PositiveOutcomes.pdf>.
- [16] S. Prema, et al. “Fingerprint Based Medical Information System.” *International Journal Of Research In Computer Applications And Robotics*, vol. Volume 2, no. Issue 4, April 2014, pp. 181-189. <https://www.ijrcar.com>, Issn 2320-7345.
- [17] “A Strong Pulse for Biometrics in Healthcare.” <http://www.planetbiometrics.com/article-details/i/1745/>, 27 September 2013.
- [18] Utzhanova, Assiya. “Fingerprint Technology and Sustainable Development.” *European Journal*, 2016, pp. 325-334.
- [19] Vedanti Suhas Mahulkar, et al. “Fingerprint Based Patient Information System.” *International Journal of Innovative Science and Research Technology*, vol. Volume 2, no. Issue 12, December– 2017. <https://ijisrt.com>.
- [20] Zuniga, Alejandro Entique Flores, et al. “Biometrics for Electronic Health Records.” *Springer Link.*, 2010, pp. 975-983. <https://link.springer.com/>, <https://doi.org/10.1007/s10916-009-9313-6>.
- [21] “Adafruit Optical Fingerprint Sensor.” <https://learn.adafruit.com/adafruit-optical-fingerprint-sensor>, 20 March 2020