

## Management patients information based finger print

Ahmed Bashar Fakhri, Huda Farooq Jameel, Mustafa Falah Mahmood

Department of Medical Instrumentation Techniques Engineering, Electrical Engineering Technical College,  
Middle Technical University, Baghdad, Iraq

### Article Info

#### Article history:

Received Jan 28, 2022

Revised Apr 10, 2022

Accepted Apr 21, 2022

#### Keywords:

Arduino UNO

Fingerprints sensor

Micro-SD card

### ABSTRACT

A fingerprint is certainly one of the distinguishing features of the human body that is easily available and identifies one individual from another. The fingerprint sensor increases this distinctiveness, which is a device that can automatically classify or identify a person. The fingerprint based medical system is a more efficient means of storing clinical data for patients. It makes take advantage of fingerprint recognition technology to quickly and easily for determine the patient's past medical history. The system consists of an Arduino UNO board, a fingerprint sensor, an secure digital (SD) card module, and a micro-SD card. The suggested technology allows the use of a micro-SD card to store patient information as well as send it by internet. When this system was compared to the manual technique, the results indicate that the main advantage is that the proposed device saves a significant amount of time that manual searching and enrolling requires. Patients' information is simply collected and managed with this system, which has enhanced dependability, durability, and efficiency. It provides improved speed and performance, as well as better data security because the data is stored within the device.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Mustafa Falah Mahmood

Department of Medical Instrumentation Techniques Engineering, Electrical Engineering Technical  
College, Middle Technical University

Baghdad, Iraq

Email: mustafa.falah@mtu.edu.iq

## 1. INTRODUCTION

Machine learning and robots have had a significant impact on how healthcare is delivered to patients. Because of developments in remote monitoring of patients and wearable technology, real-time remote medical observation has grown more powerful and adaptable. Cloud computing and wireless technology have aided significant breakthroughs in healthcare, and wireless sensor networks are now a key component of mobile technologies for e-healthcare. So, many methods are used in examines the authentication factors used in electronic health records [1].

In addition, a fingerprint-detecting device, which is used one type of sensor is used the fingerprint sensor. The precision, superior performance and resilience are the major benefits of this equipment. Both fingerprint scanners and readers are incredibly secure and appropriate devices for security rather than a secret word because the password is easy to guess and difficult to remember. A fingerprint-protected password authentication technique that does not require the secret parameter to be saved in the phone [2]. Throughout the secret key generation process, the password and fingerprint should always be submitted. The user's password is veiled whenever the computer communicates with the cellular telephone to protect it from adversarial attempts. According to theoretical and empirical research, this strategy improves the security of the person's secret. Nevertheless, the technique could persist in the opponent's dictionary, repeat, and

phishing attempts. The technique could alleviate mobile phone storage demand and is simple to implement. A confidential fingerprint authentication method was also provided, which was predicated on a totally homomorphic encryption technique in which biometric data was always maintained and analyzed in an encrypted state [3]. The proposed technique could conduct fingerprint identification by utilizing a fully functioning fingerprint authentication protocol with a raw dataset (including 4,000 samples) and the fast fully homomorphic encryption over Torus (TFHE) module. It assists in the preservation of a centralized health record file for an individual, enabling the professional to better serve the person [4].

The important information entrenching tools for protecting patient information confidentiality and privacy by concealing its presence [5]. A modified picture steganography approach was proposed in this study. The system was built with MathWorks, and dual performance measures were utilized to examine the suggested system, that included mean squared error (MSE) and peak signal-to-noise ratio (PSNR). As a result, the suggested secure medical information system when compared to other preexisting systems; the system is demonstrated to be capable of concealing medical information and making undetected stego pictures with minor entrenching falsifications contrasting approaches. A mobile device method for protecting e-health records has been presented [6]. The approach consists of security dialogues, an algorithm for granting permissions to patients as well as doctors, and administrative staff, a security analysis of the suggested authentication, an implementation file, and simulation results that demonstrate the presented approach's adequacy in terms of processing and communication as compared to other classical values methods.

The primary difficulties and challenges connected to dataset security and privacy in wireless body area networks (WBANs) are highlighted in this study [7]. They offer a hybrid data model. D-Sign is a mechanism for encrypting and decrypting data. The use of digital signatures also look into it performance of the suggested approach in comparison to the state-of-the-art procedures aimed at ensuring the safety and security in WBANs privacy is important. Despite significant security problems, this study employs cryptographic approaches with biometrics [8]. The establishment of a bio-cryptography key management strategy for protecting the privacy of patients' characteristics in a cryptographic oriented electronic health record contributes to the body of knowledge in healthcare and self-care. The system evaluation results show considerable gains as the biometrics false acceptance ratio (FAR) were considerably lowered, lowering the possibility of imposters effectively access to patients' sensitive health information. This study also validates the viability of applying fuzzy key binding schemes in real-world systems, particularly fuzzy vault, which displayed good performance in evaluation. This study includes a comprehensive literature overview and analysis of cutting-edge approaches for ensuring security and privacy in Healthcare 4.0 [9]. Also, examined the block chain-based method to provide insights into the scholarly and practitioner groups. Various classifications utilized in Healthcare 4.0 to investigate various security and privacy problems are also given in an organized manner. Finally, existing security and privacy problems and potential research initiatives in Healthcare 4.0 are outlined. Propose a biometric-based authentication mechanism to provide safe access to patients healthcare and self-care from any place primary identified different security dangers and obstacles in obtaining healthcare and self-care from the database repository in the proposal [10]. Following that, the secured biometric authentication system is constructed and certified using the automated verification of internet layer security and applications program. The results show that the proposed approach outperforms the conventional state-of-the-art methodological approaches. BAMHealth Cloud, a cloud-based system for healthcare dataset management, was recommended employing behavioral signature-based identification to ensure security of e-medical dataset access [11]. The training of signature samples for identification was done in parallel on the Hadoop map-reduce architecture using a resilient backpropagation neural network. According to proper testing, it produces an arrangement gain in speed, an energy efficiency ratio (EER) of 0.12, a sensitivity of 0.98, and a specificity of 0.95. An evaluation of the system's performance with some other algorithms demonstrates that the proposed method outperforms the existing processes in the research.

Furthermore, an innovative lightweight authentication mechanism for wearable devices an approach enables a user's wearable devices and mobile terminal was proposed that they mutually validate each other and create a digital certificate [12]. Mathematics proofs, unofficial security assessments, and formal requirements are all examples of formal specifications to show the scheme's security. The scheme's efficacy was further assessed using the NS2 simulator. A comparison showed that the proposed approach offers higher security and functionality aspects, as well as lower communication and computation costs. Established an AT&T system for controlling the patient data access control mechanism encryption is also performed via ARCANA, which enables hierarchically satisfying access to multiple data resources [13]. The access control framework is produced using the extensible access control markup language (XACML) access model. The primary reason behind selecting this design was the need to access data via AT&T in accordance with XACML standards. The encryption of medical data using multiple authorization procedures has been mandated for adequate data access control. The aforementioned may influence consumer trust in the e-health

paradigm, increasing large-scale usability. However, it is necessary to test the suggested strategy in a real-world setting. Moreover, the identity and quantity of database sources, although the causes chosen are respectable and generalizable are the most significant constraint in this survey [14]. Because of the quick expansion in this industry, it is impossible to survey on time. The emphasis was on the idea that a snapshot of scientific investigation on this significant trend of m-health applications does not relative to total the actuality of app use or effect; it just reflects the study community reaction to the trend, which seems to be the article's main purpose. In addition to this a proposed system was compared to that of other present schemes to demonstrate that by harnessing the benefits of universal serial bus (USB) and mass storage device (MSD), it is suitable for application in a smart healthcare context [15]. However, imposing on-demand security with the integration of risk-based authentication, without interfering with the simple authentication setup under common situations.

Nonetheless, a secure and lightweight remote medical verification approach of biometric - based inputs for portable healthcare situations was proposed [16]. It provides an authentication process with a data encryption agreement: i) It does not require distant location transmission of the participant's biometric data; ii) It does not maintain a dataset of interaction binding the sick people to their biometric features; iii) It should not have to analyze biometric data; vi) The mathematical cost is greatly lowered, and it prevents various attacks such as recording, fake accent, virtual machine spoofing, confidentiality, insider, man-in-the-middle, as well as cyber. Simulations are used to assess the overall feasibility of the proposed strategy. The findings point to excellent security performance. From the other hand, an identity verification system approach for remote health status monitoring has been developed, which not only addresses abovementioned issues [17]. Furthermore, using body area network (BAN) logic-based formalized security analysis is practical in determining protocol security features. The application of the augmented automated protection tool's results would analyze the security consequences of integrating with it in the context of the 5G distributed system, cloud-internet of things (IoT), and wireless body area network (WBAN). Similarly, a new lightweight authentication process for an internet-of-things real-time healthcare monitoring system has been described [18]. The suggested system should provide a high standard of protection and defense against various hazards such as cyberattacks, replay attacks, server impersonation, and eavesdropping attacks. In recent studies, writers use the automated evaluation of internet security methods and applications (AVISPA) tool to simulate the procedure to assess the performance valuation and safety research. The AVISPA tool is a simulator that is widely recognized as an excellent method of expressing the threat model. Similarly, a multiple-factor IoT-based verification solution for healthcare institutions that can securely exchange critical data via an insecure link was presented [19]. The session code TFASH's security is demonstrated by formal security analysis utilizing the mutual validation utilizing BAN principles and the results oriented recruiting (ROR) paradigm. The informal security study demonstrates that the system is resistant to various known assaults. Present a telecare medical information system (TMIS)-based protocol that is both efficient and safe and forms use of simple symmetric encryption calculations [20]. The system contributed is supported by extensive formal security analysis, and its safety properties are confirmed using the automated ProVerif tool. The comparison findings in favor of the contributed protocol are also justified by the performance evaluation. An open-source face recognition system, Open-source was installed and assessed as part of a nationally endorsed electronic health record system [21]. Patients were initially registered using face photographs and then matched using the technique. Sensitivity, false acceptance rate (FAR), false rejection rate (FRR), and failure to capture rate (FTC) were used to test the accuracy of facial recognition (FTE). The study included 103 people (mean age 37.8 years, 49.5 % female). The system gave the following outcomes: 99.0% sensitivity, 1% FAR, 0.00 FRR, 0.00 FTC, and 0.00 FTE. The use of spectacles had no impact on the performance. In addition, hospital administration should train staff on the risks, threats, policies, and recommendations that will greatly increase data confidentiality, availability, and honesty, making the electronic health records system more secure [22]. The results also show that the majority of administrative security controls, such as processes and policies, are in effect and contribute to information security. The majority of the health records employees agreed on the information security rules and procedures, and they appear to agree that they are in place and functioning properly. Unlike the administrative security control, the majority of Moi teaching and referral hospital (MTRH) employees differed on the technological and physical security controls. The fuzzy dependent decision-making with big data approach procedure for protecting healthcare information data was examined [23]. The healthcare cost and utilization project set of data is used to assess data protection. On the web, a fuzzy approach was utilized to choose healthcare information exchange. Finally, the platform's brilliance was assessed using experimental results, which reveal that fuzzy decision-making combined with a large data strategy delivers higher safety accuracy (98.64%) with a fast reaction time (47.82 ms).

This research presents a novel hospital method as well as a set of strategies for establishing access control mechanisms over personal health records (PHRs) hosted on quasi-servers [24]. Attribute-based encryption approaches were used to conceal each person's PHR record in order to enable scalability and

perfectly alright access control policies for PHRs. Satisfy protects the PHR on the quasi-server, and the Acetone–butanol–ethanol (ABE) method uses it as the primary encryption primitive. Attribute-based encryption creates data access policies depending on the characteristics of the information or the user. It allows the patient to share their PHR selectively among numerous users, encrypting the record beneath the set of characteristics without establishing all the users in the list. presents a continuous security solution for intelligent healthcare systems based on IoT and biometrics [25]. Furthermore, the incorporation of biometrics into IoT raises problems concerning the execution of a user-friendly design. As a consequence, a four-tiered Internet of Things architecture based on biometrics was proposed. Smart healthcare and the Internet of Things have resulted in the establishment of a set of standards in biometric information technologies. This article proposes a new approach for combining security mechanisms to build smart healthcare through the IoT, with a high capacity for cloud services and simplicity of use. Major advancements in smart health services may be expected to produce a more secure method of accessing IoT based on identifiers and a faster identity protocol. From the relevant literature as illustrate above there are many methods to identification the patients information like password, digital signature, and finger prints. Moreover, every methods have a disadvantage, the password and digital signature may be forgotetd. The reason for preferring biometric identification technology to traditional methods of identification is that old methods of identifying are disposed to security, unreliable, and insecure. The medical information system, which will allow for the storage of a trustworthy electronic medical record system in a database. Understand the medical history as well as the therapies that already experienced by the patient. This allows us to delicate the technique as needed to enhance availability and efficiency in a real-world deployment.

The contribution of this research are:

- a. The implementation of this research is to present fingerprint biometrics for identification patient information in a health information system (HIS). Because this data contains life-critical sensitive information, ensuring its security, privacy, and safety is an important concern.
- b. The fingerprint based medical system presents a more efficient method of storing clinical information for patients. It uses fingerprint recognition technology is simply establish the patient's prior medical history.
- c. Designed and implemented a lightweight system, verified system by using 10 samples, sent information for patients for several destination, and used Inexpensive components for system.

The rest of the paper is as shown in: Section 2 depicts the suggested device design. The module experimental configurations are introduced and defined in Section 3. Section 4 highlights the general outcomes and technique explanations. Section 5 concludes with a conclusion and a suggestion, as well as observations and ideas for further research.

## 2. METHOD

The proposed system involves fingerprint sensor, Secure digital (SD) card module, SD memory, microcontroller, and display unit such as laptop, mobile phone, external data storage, and nurse center via wireless module. First, the fingerprint sensor is acting input data from patients then process the signal in microcontroller (i.e. Arduino Uno) in analog pin for insert, modifying, and adding data. Next, SD card is used for storage, modifying, and adding data. Finally, send data to display unit via wireless module, laptop, and external data storage, as shown in Figure 1.

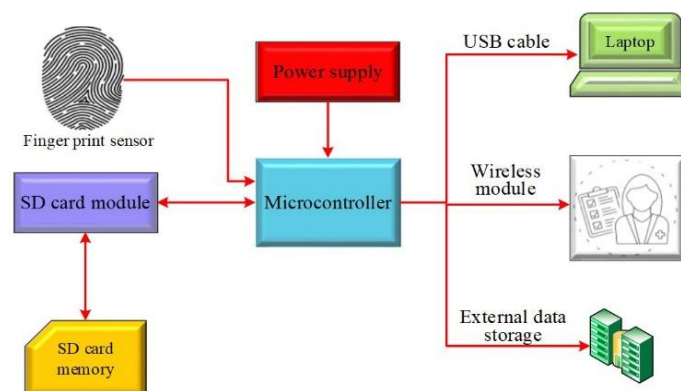


Figure 1. Block diagram for proposed system

A fingerprint sensor R307-module was employed in this study. It consists of a fingerprint scanner, a large digital signal processor (DSP), an elevated fingerprint synchronization algorithm, high-capacity flash cards, and other equipment and software elements that perform tasks such as fingerprint entrance, image analysis, feature matching, browsing, and layout storage. It has a stable performance and a simple structure [26], [27]. The SD card module is a straightforward way to transfer data to and from a normal SD card. The pinout for SD card is microcontroller-compatible. It enables you to incorporate data recording and mass storage into system. This module features a serial peripheral interface that is compatible with any SD card. In addition, power supply for this module is 5 or 3.3 V. This SD card is used in several applications such as data logger, audios, videos, and graphics [28], [29]. The microcontroller used in this work is Arduino Uno because used a processor ATmega328 [30]-[32]. The board features digital and analog (I/O) connectors that may be linked to masks and other components on the extension board. The board has digital pins and can be configured with the Arduino programming environment [33], [34]. The output device used in this paper pc, laptop, and any smart phone to display a result.

### 3. PROPOSED METHOD/ALGORITHM

The fingerprint identification system is separated into three parts: hardware, software, and network components. The hardware components are the devices that are used to connect to the server where the database is stored. The software consists of the graphical user interface (GUI), the database, which is hosted on an internet server, and additional supporting applications. Finally, the network depends on the net to send the medical information to the doctor or to another hospital. The aim of this proposed approach is to design a device stores the information of the patients attending to the clinics or hospitals and recognizes them by the fingerprint in the follow up visits.

The objective is to reduce the time of searching for the documents and get the information of the patient even if he is unconscious by the using of fingerprints. Hardware configuration involves an Arduino Uno (ATmega328 microcontroller), finger print sensor, SD card module, SD card, two buttons, and a computer, as shown in Figure 2 represents the all parts of the system. In addition, software configuration involves Arduino software, it is open-source and an integrated development environment that it is easy to write code and upload it to the board. The environment is written in Java and is based on processing and other open-source software. This software can be used with any Arduino board. (i.e. Arduino IDE 1.8.18) [34], [35]. Figure 3, illustrate a prototype hardware for propose system, in Figure 3(a), illustrate an external appearance of the proposed system. In addition, the internal appearance of the proposed system as shown in Figure 3(b). Furthermore, show the information for patients in screen monitoring such as laptop, mobile, send data to display unit via wireless module, Microsoft visual studio [36], and external data storage.

Moreover, a special algorithm for programming the microcontroller is shown in Figure 4. The mechanism of entering information is explained by entering the fingerprint in the place designated for it, and then scanning the fingerprint to compare the information about the patient through the fingerprint. The name of the new examination conducted for the patient, as this information will accumulate for one patient depending on his fingerprint. The purpose of this technique is to adopt electronic information stored in external or internal storage units, and this data can be sent electronically to the doctor in the same place or in another place.

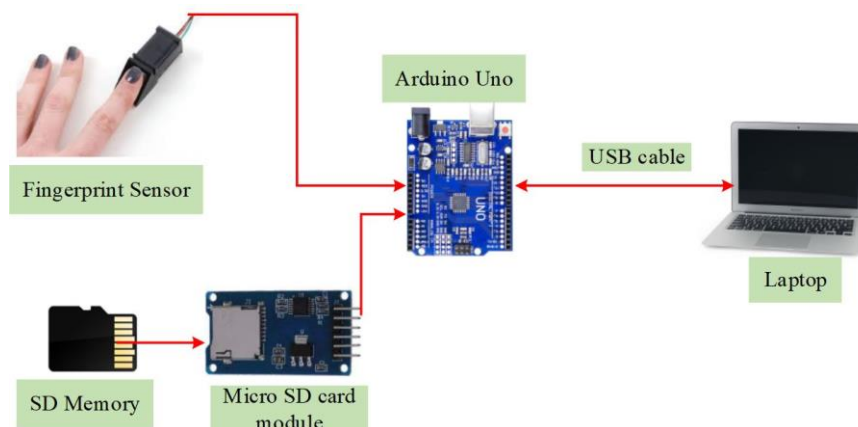


Figure 2. Circuit diagram for proposed system

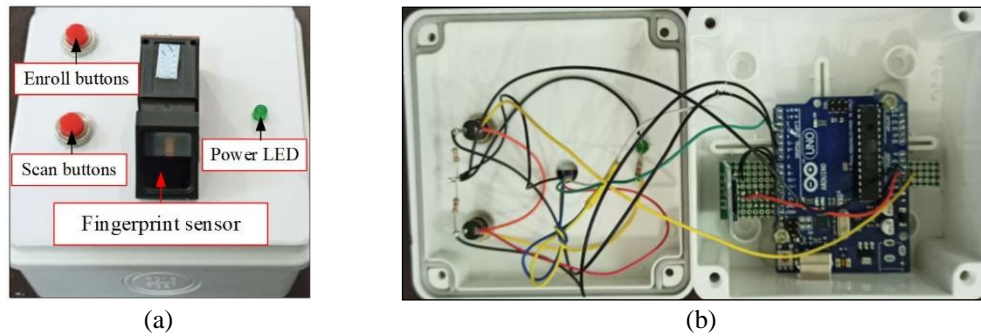


Figure 3. Snapshot for proposed system based appearance (a) external and (b) internal

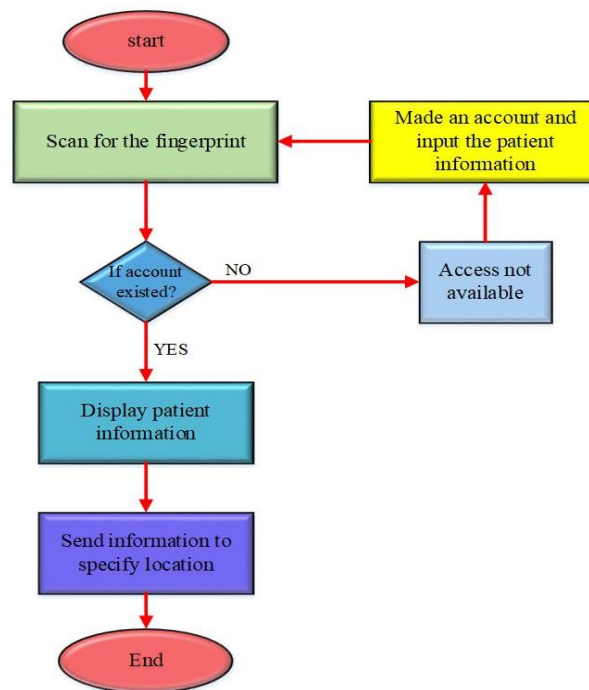


Figure 4. Algorithm for programming the microcontroller

#### 4. RESULT AND DISCUSSION

Patients' registration are classified as either Out-patient or In-Patient. The fingerprint scanner is used to acquire biometric data (during signup) or to match the patient's fingerprint to one in the database. In addition the patient receives a unique identification number after completing registration, which allows for more freedom in looking for medical information. In proposed system used serial monitoring for Arduino software to display a results. Besides, used Microsoft visual studio is an integrated development environment from Microsoft, as shown Figure 5. It is used to develop computer programs, websites, web applications, web services, and mobile applications. It can produce both essential codes and managed codes. This study has used the Microsoft visual studio to program the system, filters, DC remove, and make a GUI. In this study, this software is used to program the Arduino UNO to control finger print sensor and shows the matching prints. Also, to display the storage medical information in the data storage for each patient. Figure 6 represents parts of the codes used to program the sensor and the motor driver as shown Figures 6(a) and 6(b).

To measure a validation of the device 10 volunteers with an age range 13–60 years on different genders. Which has been inserted their medical information and tested the device in all situations. The Table 1 illustrates of the age, gender, and match ratio based correct fingerprint. We noticed in this table that some patients do not have to match the ratio because the fingerprint sensor does not read correctly because the fingerprint was effected due to their daily work or sharp tools that affect the fingerprint, so we recommend using more than one finger for the patient to facilitate the patient's ability to obtain his private information.



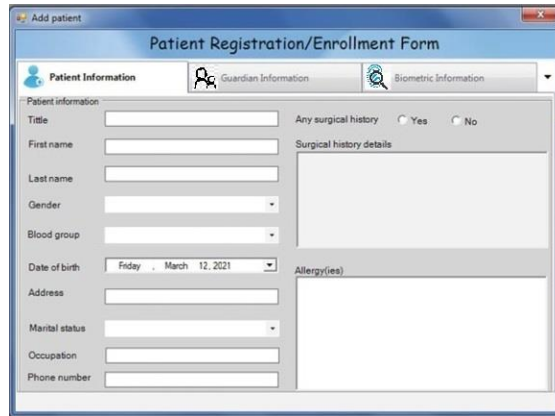


Figure 5. Snapshot for Microsoft visual studio

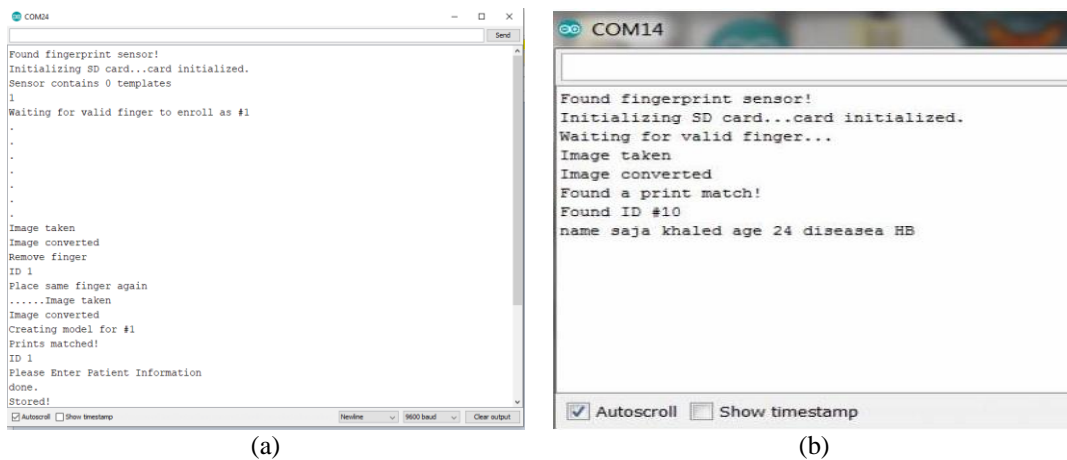


Figure 6. Parts of the codes to program the sensor and the motor driver (a) serial monitoring based enrollment mode and (b) serial monitoring based enrollment mode scanning mode

Table 1. Eexplains the validation prototype system.

No.	Age	Gender	Match ratio
1	13	M	1
2	24	F	1
3	30	F	1
4	34	M	1
5	37	M	1
6	40	F	1
7	41	M	1
8	46	F	N/A
9	55	M	1
10	60	F	N/A

\*M is male, F is female, N/A is not valuable

## 5. CONCLUSION

The purpose of this paper is to build a fingerprint sensor system to manage fingerprint data to identify each person by the fingerprint sensor. An embedded fingerprint-based patient management system using a microcontroller (i.e. Arduino UNO) was built in this study. The biometric patient management system for patients visiting clinics or hospitals was developed using Arduino. The research intended to solve the challenges that doctors experienced while storing and looking for patient information. The results of employing the established embedded fingerprint-based patient management system. The technology allows for the accurate registration of patient fingerprints and the storage of full patient history. The doctor can access the patients' saved information at any time. Even if the patient is unconscious, the fingerprint management system can recognize him/her. Future work will focus on using wireless technology for

charging and operation system without using direction power. Furthermore, saving patient information using the cloud service for easy patient access to it through phone devices or other ways.

## ACKNOWLEDGEMENTS

The authors are thankful to the Electrical Engineering Technical College at Middle Technical University in Baghdad, Iraq, for supporting them with the investigations.

## REFERENCES




- [1] M. Jayabalan and T. O'Daniel, "A study on authentication factors in electronic health records," *Journal of Applied Technology and Innovation*, vol. 3, no. 1, pp. 7–14, 2019, [Online]. Available: <https://jati.apu.edu.my/>.
- [2] C. Yang, J. Zhang, J. Guo, Y. Zheng, L. Yang, and J. Ma, "Fingerprint protected password authentication protocol," *Security and Communication Networks*, vol. 2019, pp. 1–12, Jun. 2019, doi: 10.1155/2019/1694702.
- [3] T. Kim, Y. Oh, and H. Kim, "Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption," *Security and Communication Networks*, vol. 2020, pp. 1–11, Feb. 2020, doi: 10.1155/2020/4195852.
- [4] M. Jafar Sathick Ali, J. Kaliappan, and R. Lokeshkumar, "Patient health informatics system using cloud computing and IoT," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 2162–2165, 2019.
- [5] R. O. Ogundokun and O. C. Abikoye, "A safe and secured medical textual information using an improved LSB image steganography," *International Journal of Digital Multimedia Broadcasting*, vol. 2021, pp. 1–8, Mar. 2021, doi: 10.1155/2021/8827055.
- [6] J. J. Hathaliya, S. Tanwar, and R. Evans, "Securing electronic healthcare records: A mobile-based biometric authentication approach," *Journal of Information Security and Applications*, vol. 53, p. 102528, Aug. 2020, doi: 10.1016/j.jisa.2020.102528.
- [7] A. H. Abdullah, R. A. Butt, M. W. Ashraf, K. N. Qureshi, and F. Ullah, "Securing data communication in wireless body area networks using digital signatures," *Technical Journal*, vol. 23, no. 02, pp. 50–55, 2018, [Online]. Available: <http://tj.uettaxila.edu.pk/index.php/technical-journal/article/view/757>.
- [8] C. Meinel, A. Omotosho, and J. Emuoyibofarhe, "Ensuring patients' privacy in a cryptographic-based-electronic health records using bio-cryptography," *International Journal of Electronic Healthcare*, vol. 9, no. 4, p. 1, 2017, doi: 10.1504/ijeh.2017.10003030.
- [9] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, Mar. 2020, doi: 10.1016/j.comcom.2020.02.018.
- [10] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, "Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach," *Computers and Electrical Engineering*, vol. 76, pp. 398–410, Jun. 2019, doi: 10.1016/j.compeleceng.2019.04.017.
- [11] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabir, "BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 1, pp. 57–64, Jan. 2020, doi: 10.1016/j.jksuci.2017.07.001.
- [12] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. H. Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018, doi: 10.1109/JBHI.2017.2753464.
- [13] J. Vora *et al.*, "Ensuring privacy and security in E-health records," in *CITS 2018 - 2018 International Conference on Computer, Information and Telecommunication Systems*, Jul. 2018, pp. 1–5, doi: 10.1109/CITS.2018.8440164.
- [14] A. H. Mohsin *et al.*, "Real-time medical systems based on human biometric steganography: A systematic review," *Journal of Medical Systems*, vol. 42, no. 12, p. 245, Dec. 2018, doi: 10.1007/s10916-018-1103-6.
- [15] K. Renuka, S. Kumari, and X. Li, "Design of a Secure three-factor authentication scheme for smart healthcare," *Journal of Medical Systems*, vol. 43, no. 5, p. 133, May 2019, doi: 10.1007/s10916-019-1251-3.
- [16] M. Mohammedi, M. Omar, and A. Bouabdallah, "Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 5, pp. 1527–1539, Oct. 2018, doi: 10.1007/s12652-017-0574-5.
- [17] B. A. Alzahrani, A. Irshad, K. Alsubhi, and A. Albeshrri, "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT," *International Journal of Communication Systems*, vol. 33, no. 11, p. e4423, Jul. 2020, doi: 10.1002/dac.4423.
- [18] K. Dewangan, M. Mishra, and N. K. Dewangan, "A review: a new authentication protocol for real-time healthcare monitoring system," *Irish Journal of Medical Science*, vol. 190, no. 3, pp. 927–932, Aug. 2021, doi: 10.1007/s11845-020-02425-x.
- [19] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1419–1434, Jan. 2021, doi: 10.1007/s12652-020-02213-6.
- [20] B. A. Alzahrani, "Secure and efficient cloud-based iot authenticated key agreement scheme for e-health wireless sensor networks," *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3017–3032, Apr. 2021, doi: 10.1007/s13369-020-04905-9.
- [21] S. Ampama, J. M. Kitayimbwa, and M. C. Were, "Performance of an open source facial recognition system for unique patient matching in a resource-limited setting," *International Journal of Medical Informatics*, vol. 141, p. 104180, Sep. 2020, doi: 10.1016/j.ijmedinf.2020.104180.
- [22] L. Kemboi and L. Ronoh, "Security control model for electronic health records," *International Journal of Applied Sciences: Current and Future Research Trends*, vol. 12, pp. 43–52, 2021.
- [23] B. Bai and Y. Bai, "Fuzzy based decision making approach for big data research on health information management system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3363–3371, Mar. 2021, doi: 10.1007/s12652-020-02533-7.
- [24] C. Krishnan and T. Lalitha, "Securing Healthcare data using attribute based encryption techniques in cloud environment," *European Journal of Molecular & Clinical Medicine*, vol. 7, no. 11, p. 2020, 2021.
- [25] H. Hamidi, "An approach to develop the smart health using internet of things and authentication based on biometric technology," *Future Generation Computer Systems*, vol. 91, pp. 434–449, Feb. 2019, doi: 10.1016/j.future.2018.09.024.






- [26] M. Pardede, E. Hutajulu, and R. Sirait, "Laboratory room control access and monitoring system using fingerprint and XBee Pro S2C," *Jurnal Mantik*, vol. 4, pp. 1921–1928, 2020, [Online]. Available: <http://iocscience.org/ejournal/index.php/mantik/article/view/1035>.
- [27] A. K. Vaisakh, K. V. Ganesh, S. Suresh, L. Vincent, P. T. Thobias, and I. P. Nair, "IoT based intelligent public ration distribution," in *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*, Jul. 2019, pp. 1894–1897, doi: 10.1109/ICCES45898.2019.9002095.
- [28] G. Jin, K. Bai, Y. Zhang, and H. He, "A smart water metering system based on image recognition and narrowband internet of things," *Revue d'Intelligence Artificielle*, vol. 33, no. 4, pp. 293–298, Oct. 2019, doi: 10.18280/ria.330405.
- [29] D. Kumar, P. Kumar, and A. Ashok, "Introduction to multimedia big data computing for IoT," in *Intelligent Systems Reference Library*, vol. 163, 2020, pp. 3–36.
- [30] H. F. Jameel, S. L. Mohammed, and S. K. Gharghan, "Electroencephalograph-based wheelchair controlling system for the people with motor disability using advanced brainwear," in *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, Oct. 2019, vol. October-20, pp. 843–848, doi: 10.1109/DeSE.2019.00156.
- [31] M. A. Hoque, T. Islam, T. Ahmed, and A. Amin, "Autonomous face detection system from real-time video streaming for ensuring the intelligence security system," in *2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS 2020*, Mar. 2020, pp. 261–265, doi: 10.1109/ICACCS48705.2020.9074260.
- [32] A. B. Fakhri, S. K. Gharghan, and S. L. Mohammed, "Power reduction based on sleep/wake scheme in wireless sensor network for patients vital sign monitoring system," *Power*, vol. 62, no. April, 2020.
- [33] D. P. Sangeetha, S. Vijayashaarathi, A. Kaur, N. Bavya, and M. Janani, "Dynamic traffic light switching based on traffic density," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 5, pp. 1964–1972, 2021.
- [34] M. F. Mahmood, S. K. Gharghan, S. L. Mohammed, A. Al-Naji, and J. Chahl, "Design of powering wireless medical sensor based on spiral-spider coils," *Designs*, vol. 5, no. 4, p. 59, Sep. 2021, doi: 10.3390/designs5040059.
- [35] M. F. Mahmood, S. L. Mohammed, S. K. Gharghan, and S. L. Zubaidi, "Design and implementation of wireless power transfer for wireless heart rate monitoring system," in *Proceedings - International Conference on Developments in eSystems Engineering, DeSE, Dec. 2020*, vol. 2020-December, pp. 453–458, doi: 10.1109/DeSE51703.2020.9450792.
- [36] E. A. Salako, "Design and implementation of a fingerprint-based platform for securing electronic voting system," Thesis, Federal University of Technology Akure, 2021.

## BIOGRAPHIES OF AUTHORS






**Ahmed Bashar Fakhri**    received his B.Sc. in Medical Instrumentation Techniques Eng. from Middle Technical University, Iraq in 2007. He is with the Department of Medical Instrumentation Engineering Techniques, Electrical Engineering Technical College, Middle Technical University, Baghdad-Iraq, as Technical Engineer. In 2019 he has a mater degree Tech. in Medical Instrumentation Engineering Techniques, from Electrical Engineering Technical College, Baghdad-Iraq. He interested in medical device, wireless sensor network, measurement accuracy, and statistical analysis. He can be contacted at email: [ahmed\\_bashar@mtu.edu.iq](mailto:ahmed_bashar@mtu.edu.iq).



**Huda Farooq Jameel**    received her B.Sc. in Medical Instrumentation Techniques Eng. from Middle Technical University, Iraq in 2006. She is with the Department of Medical Instrumentation Engineering Techniques, Electrical Engineering Technical College, Middle Technical University, Baghdad-Iraq, as Technical Engineer. In 2020 she has a mater degree Tech. in Medical Instrumentation Engineering Techniques, from Electrical Engineering Technical College, Baghdad-Iraq. She interested in controlling medical device, image processing, and signal processing. She can be contacted at email: [huda\\_baban@mtu.edu.iq](mailto:huda_baban@mtu.edu.iq).



**Mustafa Falah Mahmood**    received his B.Sc. in Medical Instrumentation Techniques Eng. From Middle Technical University, Iraq in 2010. He is with the Department of Medical Instrumentation Engineering Techniques, Electrical Engineering Technical College, Middle Technical University, Baghdad-Iraq, as an Assistant teacher. Has MSc degree in Medical Instrumentation Engineering Techniques, from Electrical Engineering Technical College, Baghdad-Iraq in 2020. Interested in research including wireless energy transfer, alternative power production without the need of batteries, the creation of low-cost, elevated medical devices, medical sensors, and electronics applications. He can be contacted at email: [mustafa.falah@mtu.edu.iq](mailto:mustafa.falah@mtu.edu.iq).