



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 6, June 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.118



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Secure Sharing of Health Record Using Biometric Authenticity

Nikhil Dighe¹, Mayuri Dighe², Kishori Bhalerao³, Abhishek Dhekane⁴, Prof. S. B. Kawade⁵

U.G. Student, Department of E & TC, AVCOE, Ahmednagar, Maharashtra, India¹

Associate Professor, Department of E & TC, AVCOE, Ahmednagar, Maharashtra, India²

ABSTRACT: Personal Health Records (PHRs) is used to increase the interoperability between healthcare organizations and patient health information while preserving privacy and confidentiality of patient information. PHR is structured information that may include text, image(s) or both of them; its aims to have the features of decentralization, security, openness, and traceability. This systematic review aims to examine and identify the forms of implemented Personal health records with the available protection and privacy techniques. PHR could be enhanced by applying the processes of authentication, authorization, and access control in security, in addition to applying privacy for both information and image included in PHR. In the similar lines, some of the hospitals are exploring the use of fingerprint scanners for patient identification and accessing their personal health record. The system is designed for providing privacy and secrecy of sharing the PHR's through fingerprint authentication.

KEYWORDS: Health Care, privacy, security, PHR, authentication, fingerprint Scanner.

I. INTRODUCTION

In the Healthcare industry, when it comes to Patient Safety and Security, the most debated and talked about subjects are Patient Identification and Patient Data Integrity. Fingerprint Recognition Technology has become part of our daily lives. Few of its most common uses are, timekeeping systems for payroll purpose and Smart-phones with the ability to identify users based on their finger prints. In the similar lines, some of the hospitals are exploring the use of fingerprint scanners for patient identification and accessing their personal health record. Cloud computing has emerged as an important computing paradigm to offer pervasive and on demand availability of various resources in the form of hardware, software, infrastructure, and storage. The cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers. Numerous methods have been employed to ensure the privacy of the PHR stored on the cloud servers. The privacy preserving approaches make sure confidentiality, integrity, authenticity, accountability, and audit trail. Confidentiality ensures that the health information is entirely concealed to the unsanctioned parties, whereas integrity deals with maintaining the originality of the data, whether in transit or in cloud storage. Authenticity guarantees that the health-data is accessed by authorized entities only, whereas accountability refers to the fact that the data access policies must comply with the agreed upon procedures. We present a methodology called Secure Sharing of PHRs in the Cloud to administer the PHR access control mechanism managed by patients themselves. The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users.

Paper is organized as follows. Section II describes automatic text detection using morphological operations, connected component analysis and set of selection or rejection criteria. The flow diagram represents the step of the algorithm. After detection of text, how text region is filled using an inpainting technique that is given in Section III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. RELATED WORK

Pieter Van Gorp Marco Comuzzi, "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud", IEEE Journal of Biomedical and Health Informatics (Volume: 18, Issue: 1, Jan. 2014). In this paper, authors presented MyPHRMachines, a novel PHR system. Leveraging virtualization techniques, MyPHRMachines allows patients to build lifelong PHRs. The records can be shared by the patient with any stakeholder interested in those. MyPHRMachines allows also the controlled sharing of application software that is required to view and/or

analyze health records. Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems. Michael S. Dohan, Mohamed Abouzahra and Joseph Tan, "Mobile Personal Health Records: Research Agenda for Applications in Global Health", [2] IEEE, 47th Hawaii International Conference on System Science, 2014. This paper discusses six research areas in which mPHRs are applied to global health issues. These research areas are: applications that are disease specific and otherwise; ensuring local relevance of initiatives; using mPHRs for the collection of data for epidemic intelligence; innovative devices and infrastructures; integration with other technologies; and issues with global health initiatives that can apply these technologies. Despite the challenges with mPHRs, they remain a viable option for addressing the various global health concerns of today. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system", [3] Journal of Computer and System Sciences, 2017. In this paper, authors proposed a general framework of secure sharing of PHRs. The system enables patients to securely store and share their PHR in the cloud server to their carers or family members. Treating doctors can further refer the patient's medical record to specialists for research purposes, while the patient's personal information remains private. In addition, cross domains operations can be supported. They provided a concrete instantiation of system. They also gave a simulation result for it. Mazhar Ali, Member, Saif U. R. Malik, Samee U. Khan, "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party" [4], IEEE, 2015. The authors (a) implement a working prototype of DaSCE and evaluate its performance based on the time consumed during various operations, (b) formally model and analyze the working of DaSCE using High Level Petri nets (HLPN), and (c) verify the working of DaSCE using Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The results reveal that DaSCE can be effectively used for security of outsourced data by employing key management, access control, and file assured deletion. Assad Abbas, Samee U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", [5] IEEE 2014. This paper aimed to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds. Moreover, the privacy preserving approaches are classified into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted.

III. METHODOLOGY

A) Block Diagram:

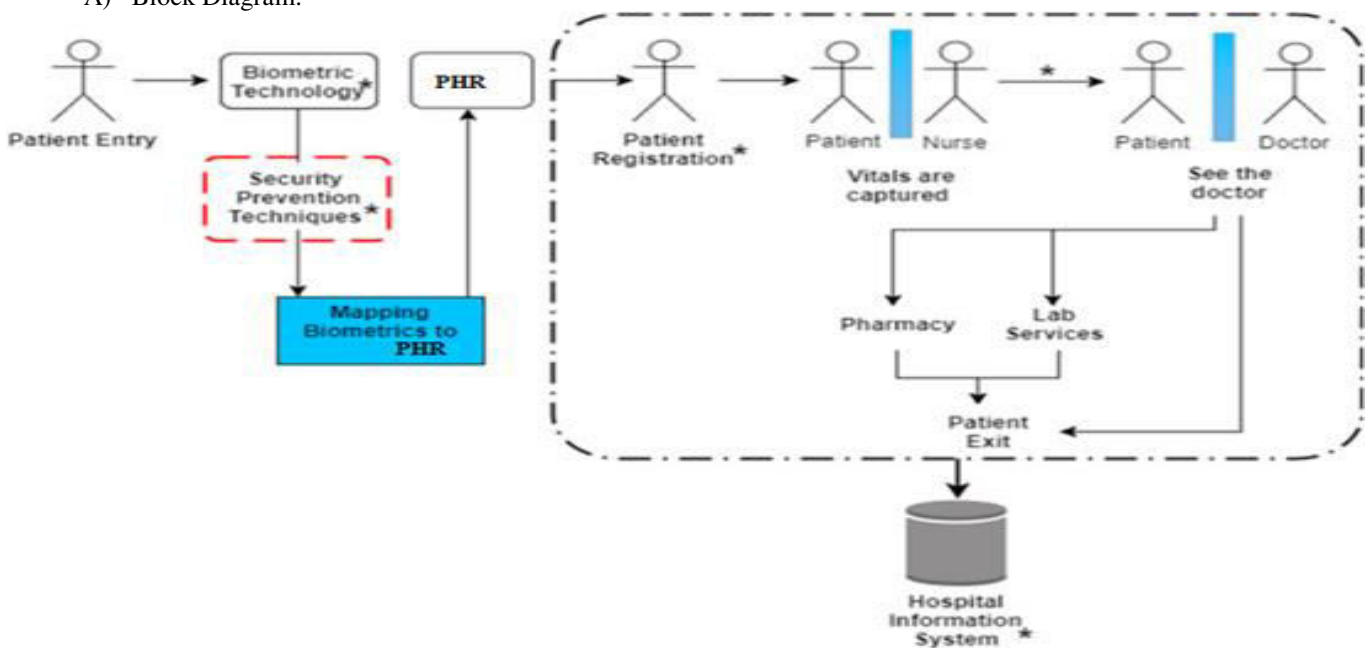
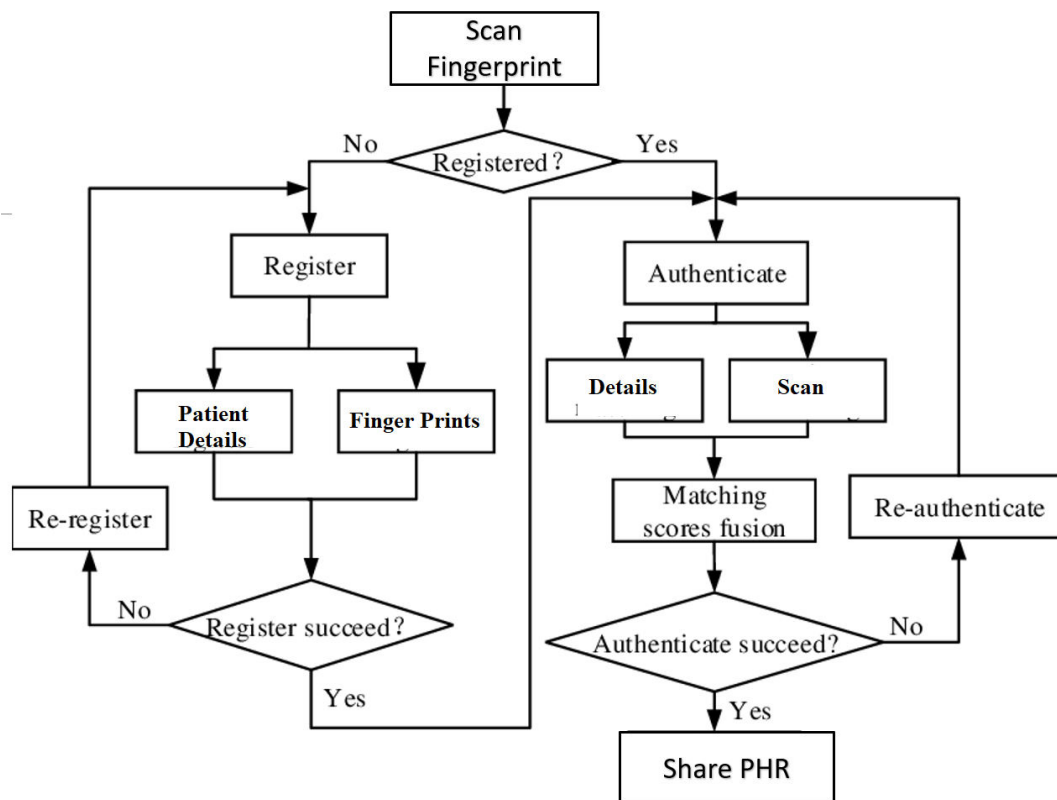


Fig 1: Block Diagram.

B) Block Diagram Description:

1. When a patient registers at the hospital, he is required to scan his finger on a fingerprint scanner and provide some associated personal information.
2. This enrolment process helps the patient on his follow ups, as on each successive visit his fingerprint scan will be compared with the pre-scanned image in the hospital's database.
3. Thus, eliminating the need to check the patient's credential on paper and provide a quick access to his/her personal and medical information. The quick and accurate access to the medical history also reduces the chances of wrong diagnosis and medication.
4. Further, the fingerprint door lock would restrict the entry of unregistered members and enhance the security measure.
5. Another important implementation of fingerprint scanner in hospitals is during the emergency admissions.
6. Even if a patient arrives in an unconscious state, a simple finger scan can help identify the patient and provide access to the patient's medical history.
7. After a finger scan, the fingerprint image is sent to the main system for verification.
8. If it is authorized, the requested information is delivered to the patient.

C) Flowchart



D) Algorithm:

AES algorithm helps to encrypt the PH. The algorithm uses 10 or 14 rounds for encryption with given key depending on 128 bytes or 256 bytes respectively. Each Round consist of 4 steps which includes Sub Byte where one each byte is substituted with another byte. The next is row shifting where whole row is shifted. Next is mix column where columns are mixed and the last one is adding round key.

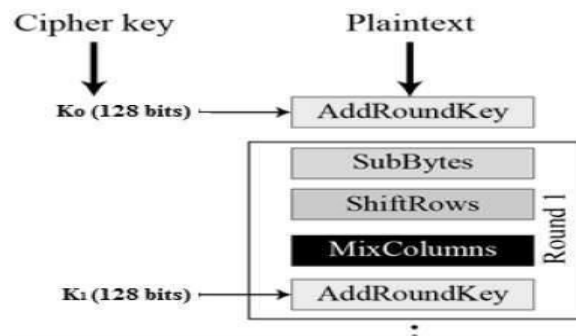
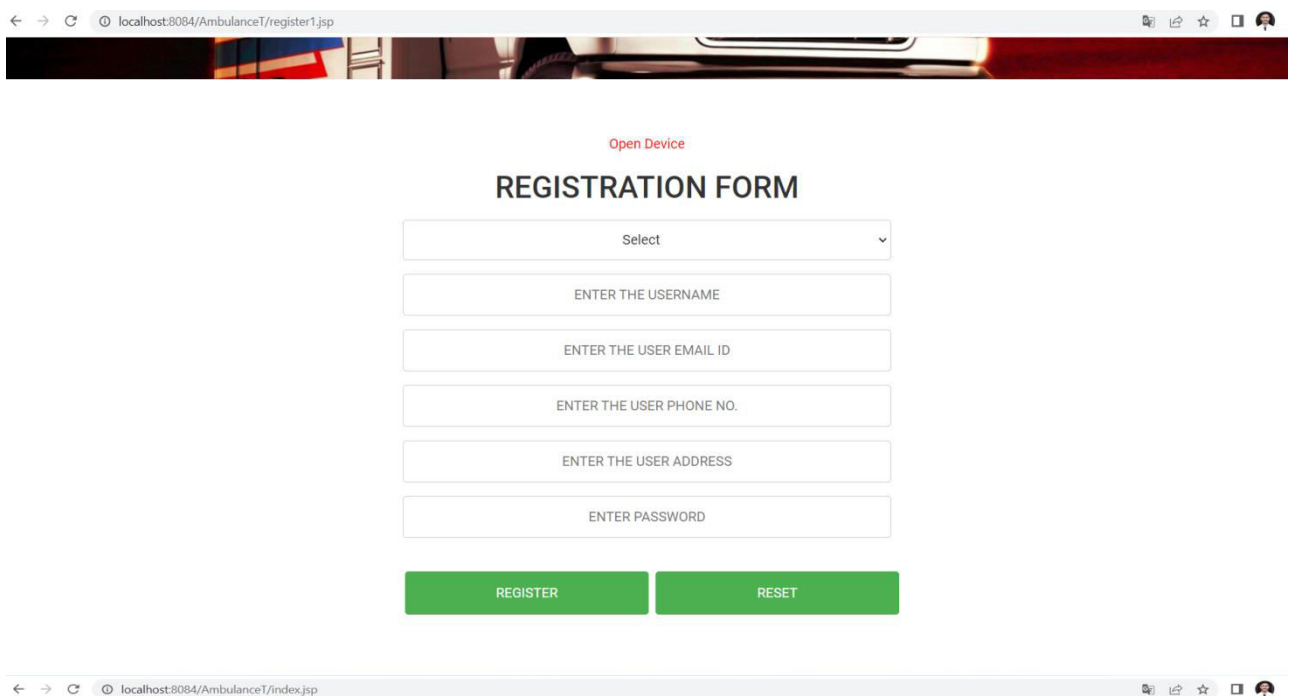


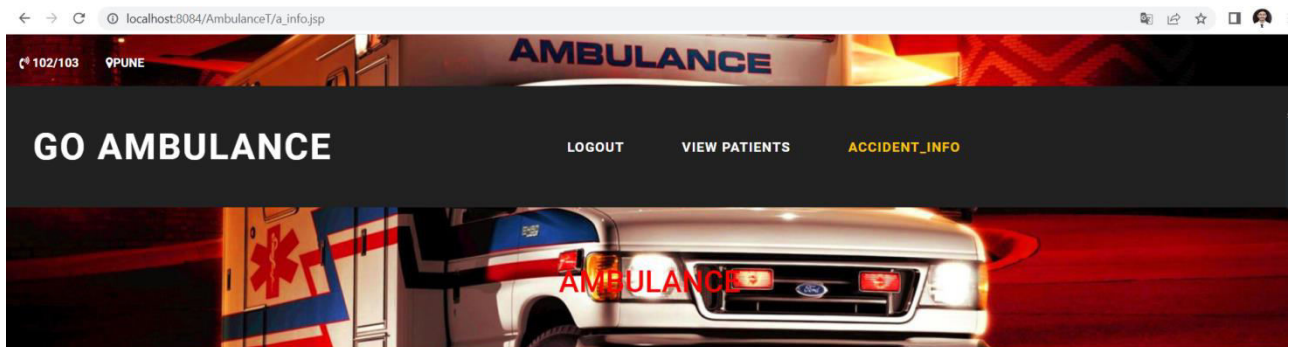
Fig 2: AES

IV. EXPERIMENTAL RESULTS



THUMB

We can use fingerprint for getting person information like name, blood group, previous medical history etc. By using thumb impression we can get patients information easily. Some accident person body not identified in this situation by using thumb impression we can find out person information.



[Open Device](#)

Search Patient

Ambulance Id
location coordinates(,)
Find Patient
RESET



PATIENT FORM

Patient Name :	Dinesh Ubale
Mail-ID :	dinesh@gmail.com
Contact No :	7350456969
Permanent Address :	Pune
Gender :	male
Blood Group:	O+ve
Age :	22
Height(Inches) :	170
Weight(Kg) :	62
Body Mass Index :	healthy
Body Temperature(degree C) :	38
Pulse Rate(Per Minute) :	78



V. CONCLUSION

System will be developed to provide secure sharing of personal health record across different hospitals under bio-metric authentication. Fingerprint is used for bio-metric as it is unique and easy to access even in emergency situation..

REFERENCES

- [1] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multichannel communication in Edge-of-Things", Future Generation Computer Systems, 2018.
- [2] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech", Journal of Network and Computer Applications, 2017.
- [3] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system", Journal of Computer and System Sciences, 2017.
- [4] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, Future Generation Computer Systems, 2015.
- [5] Assad Abbas, Samee U. Khan, Senior Member, "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.
- [6] J. Li, "Electronic personal health records and the question of privacy", Computers, 2013.
- [7] Swatee S. Nikam, Jyoti P. Kshirsagar "Implementation of secure sharing of PHR's with IoMT cloud" in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, (2019).
- [8] Pieter Van Gorp and Marco Comuzzi, "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud", IEEE 2014



INNO  SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118



ISSN  INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details