International Journal of Recent Development in Computer Technology & Software Applications
http://eurekajournals.com/IJRDCTSA.html
ISSN: 2581-6276

Biometric Based Patient Record Management

Sonia Roy, Neelam Trivedi

Abstract

Biometrics based patient record management aims to replace the redundant and tedious patient records management systems. When a patient visits a doctor, he/she needs to carry previous reports and prescriptions. These records may get misplaced or destroyed. Our system aims to provide a platform where all these records can be stored and updated whenever required by the doctor and the patient. The doctor will be provided with an environment where he will be able to add, remove and update records and the patient will be able to view them whenever required. Medical records are personal details and need to be kept confidential and if mixed with someone else's records may have fatal consequences. For this reason, the proposed system is using fingerprint for matching a patient with his/her records. The patient will have a separate app that will allow to view the prescription and also provide methods to order the medicines.

Keywords: Biometric Based Patient Record Management (BBPRM), False Acceptance Rate (FAR), False Rejection Rate (FRR), Uniform Resource Locator (URL), JSON Web Token (JWT).

Introduction

Biometrics based patient record management (BBPRM) makes the process of managing the records of a patient simple. The patient need not carry his/her records, prescriptions and other reports. This also eases the task of managing the records on the doctor‟s part. The system will allow the doctor to view, update and the delete the records of the patients. The doctor will be able to easily modify the prescriptions, access old records and the chances of records getting mixed up are reduced to the minimum. Forthe doctor to modify a patient‟s records both the doctor and the patient will have to be authenticated. Literature survey reveals that such systems have helped in saving lives in critical situations, like in case of an accident where patient's records are not available but can be viewed with the help of systems similar to this as mentioned in the papers titled, "A novel and efficient user access control scheme for wireless body area sensor networks" [6], "Health monitoring using mobile web services" [7] and "Data security and privacy in wireless body area networks" [8].

The healthcare industry is also understanding the benefits of digitizing records. More and more healthcare systems and organisations are migrating to computerized health records. This

leads to various concerns as to how we can manage data integrity more efficiently in order to ensure that it is free from any form of corruption and unwanted modifications. A large increase in the number of electronic records has led to an increased possibility of data corruption. Additionally, as there has been an exponential growth in these systems, they tend to become more and more complex resulting in increase in the number of vulnerabilities. Compromises to data integrity cannot be made in healthcare industry as they might become the difference between life and death.

A major concern with maintaining data integrity is to implement a consistent approach across the system to facilitate proper information to matching patients with their data. The users involved in the system i.e. the doctors as well the patients should trust each other that the data provided and stored is complete, secure and safe.

In this paper we present a new low cost and efficient patient record management system. For authentication we will use fingerprint matching technique. The records of the patients will be stored on the cloud which will allow for easy availability to authorized users.

Our Contributions and Goals:

- We present a new robust, secured system that by using existing fingerprint authentication techniques allows for secure login.
- The records will be stored on cloud for easy access.
- The patient can view his/her records using the system.
- The patient will be able to view the prescription and order medicines
- The login of both patient and doctor will be required for updating records.
- Through the security verification using fingerprint, we prove that the proposed scheme achieves unconditional security.

Literature Survey

Review of Existing Systems

A number of patient record management systems that make use of password as authentication for patient records exist. However, a lot more researches on techniques for fingerprint biometrics are desirable in literature, particularly those that integrates more than one factor authentication scheme. Some of the biometrics based HIMSs are discussed in this section.

The study according to the paper titled „Biometric Access Control for e-Health Records in Pre-hospital Care.“ [1] exploited biometric identification to access a centralized health database with privacy policies. The research implemented a real-world scenario in which an ambulance gets to an unconscious patient who is in need of medical care for which their health record is retrieved from the database and is adapted to meet the requirements of privacy policies. The results of the conducted research showed a time of 19.8 seconds on an average when several patients are registered in the database.

In the research by the papers “Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services” [2] and “Alternative Biometric as Method of

Information Security of Healthcare Systems". [5], a number of Telemedicine, eHealth and Wellness (TEW) systems, analysed their technologies. Moreover, their security implementations were also investigated. The conclusions of the research stated that the wireless sensor-based systems have focused more on engineering issues of making the technology function as per the expectations, but, at the expense of security. The resellers learnt that even those systems that have implemented formidable security mechanisms may not have modelled suitable threats. The research in the paper titled "Biometric authentication system to protect sensitive medical data". [3], integrated the use of dual fingerprint and face authentication for securing patient records on Personal Computer (PC).

Biometric Technologies

The decision to select the appropriate technology in biometrics depends on a number of factors like the type of users who will interact with the system, overall cost of the system and its capabilities, the type of environment in which the system will be deployed and many more factors. In order to compare the various biometric technologies, we can construct a table consisting of the different technologies and various characteristics. Rating is based on values such as High, Medium and Low denoted by H, M and L respectively. Accuracy plays a very crucial role in the selection of the appropriate biometric technology. Confirmation regarding the identity of the user depends on a similarity score which is obtained on comparing biometric template to the captured template. Usually, the threshold for this similarity score is set to be in a certain acceptance range as measured by the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

- The False Acceptance Rate indicates the likelihood that a biometric system will incorrectly verify an individual or accept an imposter.
- The False Rejection Rate indicates the likelihood that a biometric system will reject the correct person.

As we have reviewed the existing systems and their pros and cons, we now can focus on developing a system that tries to inculcate the benefits of each, and at the same time ensure that problems faced by the existing systems are dealt efficiently so that the resulting system may fare better than the current ones.

Table 1: Comparison of Biometric Technologies

Biometric Identifier	Maturity	Accuracy	Uniqueness	Failure-to-Enroll Rate	Record Size	Universality	Durability
Face	M	M	M	L	H 84-2,000	H	M
Fingerprint	H	H	M	L-M	M 250-1,000	M	M
Hand	M	L	L	L	L 9	M	M
Iris	M	M	H	L	M 688	M	H
Signature	L	L	M	L	M 500-1,000	M	M
Vascular	M	M	H	L	M 512	H	H
Voice	L	L	M	M	H 1,500-3,000	H	L

The Proposed System

The proposed system acts in the following manner, the system administrator can add or remove doctors. A doctor can view records of patients but can only edit the records of his patients after authentication of that respective patient. Moreover, doctors can register new patients into the system and can also modify records of his /her patients. In the application available for patients, the patient can login through the app after authentication through One Time Password (OTP) inorder to view his/her records. The user cannot modify, add or delete records as they are meant only for viewing purposes. Additionally, the patient can order medicines mentioned in the prescription from online stores. This functionality is provided through Optical Character Recognition, often abbreviated as OCR which is a mechanism which will convert the handwritten text from the prescriptions to machine encoded text.

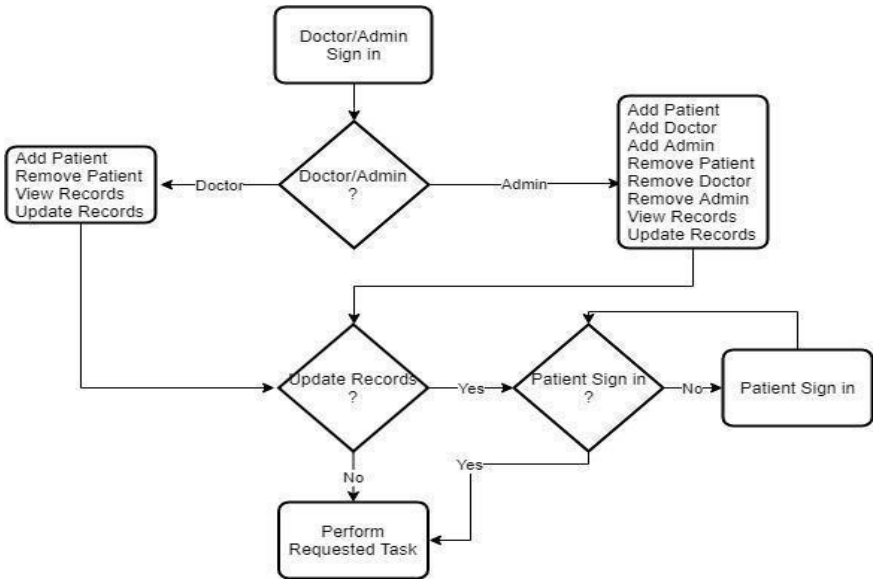

Figure 1: Work flow of doctor/admin app

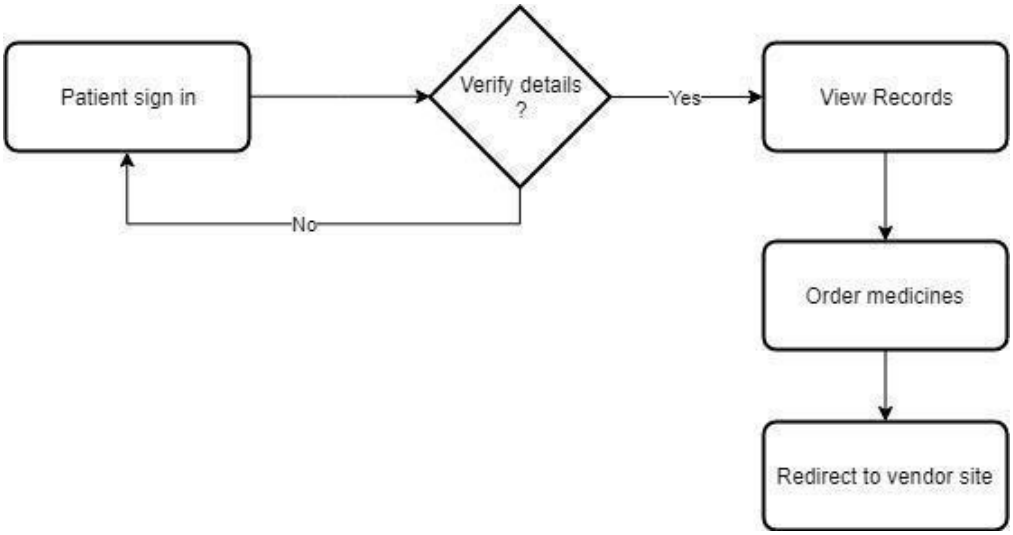

Figure 2: Work flow of patient app

Fingerprint Capturing

After the reader is initialized, a fingerprint image can be captured. Captured fingerprints are 256 grey-level images, and image width and height can be retrieved. The unique features are then extracted from the biometric sample to create the user‟s biometric template. The template is also encrypted during the creation process so as to maintain security. This biometric template is stored in a database for later use during a matching process.

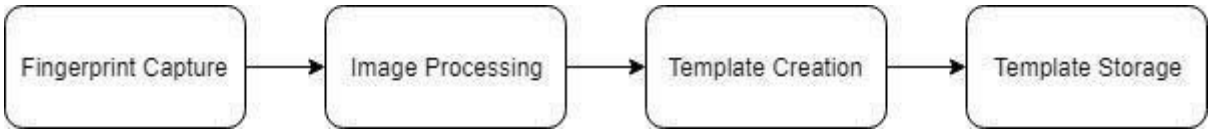

Figure 3: Fingerprint Capturing

Creating A Template

To register or verify a fingerprint, a fingerprint image is first captured, and then feature data (minutiae) is extracted from the image into a template. Minutiae are the unique core points near the centre of every fingerprint, such as ridges, ridge endings, bifurcations, valleys and whorls. The template is also encrypted to provide security.

Fingerprint Matching

Templates are matched during both registration and verification processes. The minutiae data from each image sample can then be compared against each other (i.e. matched) to confirm the quality of the registered fingerprints. This comparison is analogous to a password confirmation routine that is commonly required for entering a new password. During verification, newly input minutiaedata is compared against registered minutiae data. Similar to the registration process, verification requires the capture of a fingerprint image followed by extraction of the minutiae data from the captured image into a template.

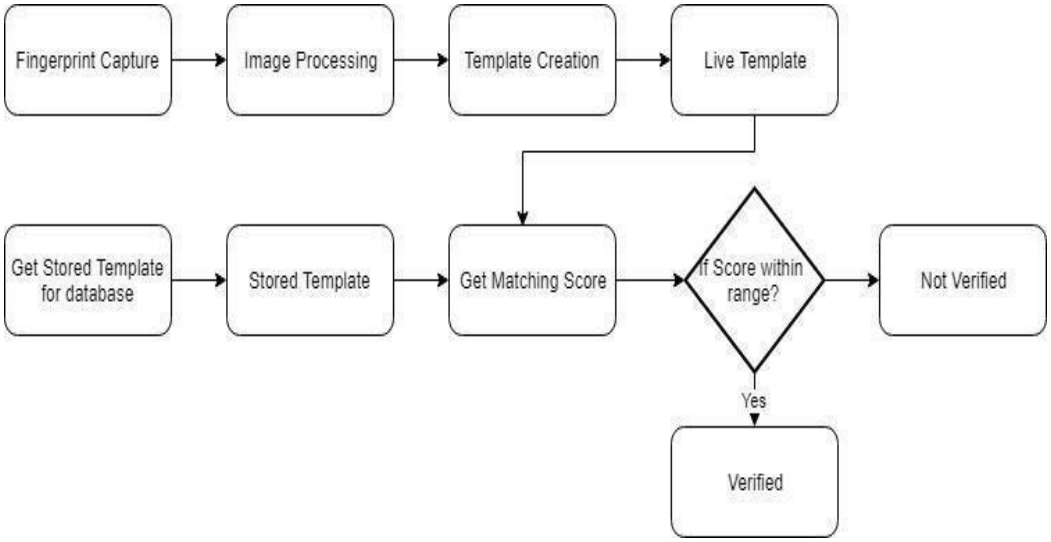

Figure 4: Fingerprint Matching

Access Control List

The access control list is a list that consists of users and the permissions/ actions that a particular user can perform.

Table 2: Access List

Action / Users	Add Patien t	RemovePatient	View Records	Update Records
Admin	Yes	Yes	Yes	Yes (only if the patient is logged in)
Doctor	Yes	Yes (only his own patients)	Yes (only his own patients)	Yes (only if the patient is logged in)

Table 3: Access List Additional Actions

Action /Users	Add Doctor	Add Admin	RemoveDoctor	RemoveAdmin
Admin	Yes	Yes	Yes	Yes
Doctor	No	No	No	No

Security Analysis

Token Based Authentication

A token is a piece of data that has no meaning or use on its own, but combined with the correct tokenization system, becomesa vital player in securing your application. Token based authentication works by ensuring that each request to a server is accompanied by a signed token which the server verifies for authenticity and only then responds to the request.

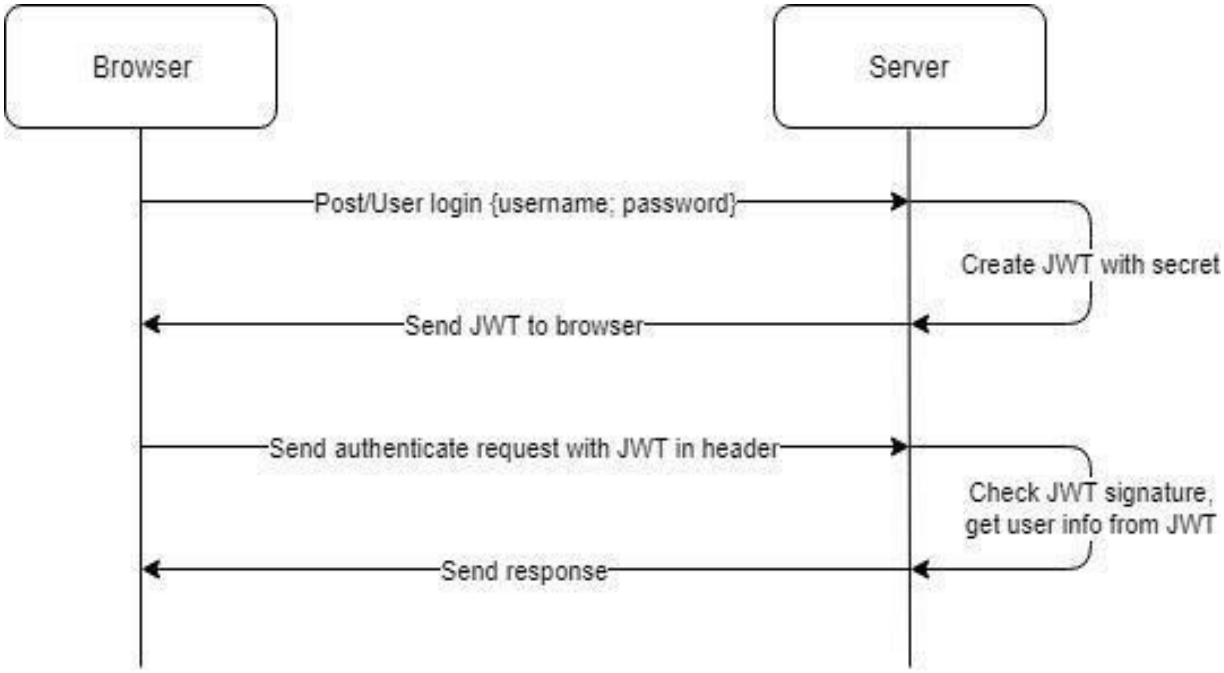

Figure 5: Token based authentication

When doctor/admin logs in into the system, a token will be assigned to him/her which will be valid for one hour. Requests thatonly the doctor or admin can send, will require the token to be verified. The token will be sent along with the request in the header.The authorization of the user, will require the current timestamp along with a secret key that the server will know. When a request is made to the server, the content that is sent to the server is the request URL, the current timestamp and hash of the currenttimestamp, the request URL and the secret key in case of doctor/admin even the token. When the server gets this request, it will extract the URL, the timestamp, the token (in case of doctor/admin) and the hash code. It will use the timestamp, URL, token (onlyin case of admin/doctor) and the secret key which it knows to generate a hash. If both the hash generated and the hash received are the same then it is a valid user and is allowed to use the services.

A major aspect while developing such systems is to ensure that it is safe from various kinds of threats and attacks that may lead to loss of data, unwanted access to confidential information and loss of data integrity. While developing the system we have incorporated certain mechanisms to prevent any kind of attacks and threats to the system.

Mentioned below are some of the attacks the system may be vulnerable to, along with the counter measures designed for the same.

Replay Attack

A replay attack is a type of an attack in which valid data is transmitted to the receiver after some interval of time for malicious reasons. Let‟s assume that an attacker intercepts the request that is sent from a user to the server and tries to retransmit. When such a request is received by the server will extract the information and check for the timestamp, but this will be an older timestamp (Ts>15) as a result the request will be rejected.

Impersonation Attack

An impersonation attack is a type of attack in which the attacker tries to gain access to the system by acting to be a valid user. If an attacker tries to gain access using such a type of attack the attacker will also require the secret key. Without the secret key the attacker will not be able to get any information from the server.

Man in the Middle Attack

In man in the middle attack the attacker intercepts the requests and responses from the client and server. However, the transmission of any data between the server and the receiver will be encrypted. Hence any data intercepted will be worthless. Additionally, for any requests the attacker wants to make to the server, the attacker will require the secret key.

Conclusions

Latest technologies are currently being used for various applications and one such booming sector is the healthcare sector. BBPRM aims to reduce the inefficient process of manual patient record management, which has many flaws. It aims to make the whole process of patient record management seamless for the doctors as well as for the patients.

The advantage of using fingerprint authorisation in the system is that it uses characteristics of the human body for identifying a particular individual thus eliminating the need to provide an identity proof at the time of registration. Also, ID proofs sub mitted may be bogus, but, the fingerprint template captured at the time of registration will be genuine. This eliminates any possibility of creating duplicate medical records and also ensures that proper care is delivered to the appropriate patient. It also provides a better solution to uniquely identify patients having same names and/or credentials thus ensuring that the data accessed during a patient‟s visit is not of any other individual.

BBPRM uses cloud storage as it provides easy server management and also proves to cost effective than maintaining local databases. Moreover, the system uses advanced mechanisms for securing the data stored as well as providing secure communication between the server and the system. Thus, the system provides a better alternative to managing patient records.

References

J. R. Diaz-palacios, V. J. Romo-Aledo, and A. H. Chinaei. Biometric Access Control for e-Health Records in Pre-hospital Care. EDBT/ICDT, March 18-22 2013, Genoa, Italy.

D. P. Mirembe. “Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services”. Master‟s thesis delivered to Radboud University Nijmegen Security of Systems.2006.

O. A. Esam, S. M. Ngwira, and T. Zuva. “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 VolI, IMECS, March12-14-2014, HongKong.

V. I. Ivanov, P. L. Yu, and J. Baras, "Securing the communication of medical information using local biometric authentication and commercial wireless links. Proceedings of the 14th International Symposium for Health Information Management Research at Kalmar in October 2009. Health Informatics Journal 16(3), pp. 212-223.

E. Andreeva. "Alternative Biometric as Method of Information Security of Healthcare Systems". Proceeding of the 12th conference of fruct association Department of information security Technologies, pp.210-214.2012.

S. Chatterjee, A.K. Das, and J.K. Sing. "A novel and efficient user access control scheme for wireless body area sensor networks", Journal of King Saud University Computer and Information Sciences, 26(2),(pp.181201), 2013.

K.Elgazzar, M. Aboelfotoh, P.Martin, and H.S. Hassanein.Ubiquitous health monitoring using mobile web services", In: Proceedings of the 3rdinternational Conferenceon Ambient Systems, Networks and Technoogies, (pp.332-339), 2012.

M. Li, W. Lou, and K. Ren. "Data security and privacy in wireless body area networks", IEEE Wireless Communications, 17 (1), (pp. 5158), 2010.