

# Cloud based Secure Multi Owner Hospital Management System

Omkar Warghade<sup>[1]</sup>, Rupashree Pandithurai<sup>[1]</sup>,  
Swarali Joshi<sup>[1]</sup>, Rutuja Patil<sup>[1]</sup>  
Student<sup>[1]</sup>,  
Department of Information Technology,  
Pune University,  
Pune, India. 411033.

Archana Jadhav<sup>[2]</sup>  
Faculty<sup>[2]</sup>,  
Department of Information Technology,  
JSPM's RSCOE,  
Pune, India, 411033.

**Abstract:-** Nowadays, in the Healthcare sector, digitalization is an essential part of the system. Technology has placed at the disposal of the healthcare community various potent tools to improve patient care. Since e-Health Records are easily available to physicians, they can access complete medical histories of patients and make the most well-considered medical decisions. Still, storing confidential health information to cloud servers is prone to revelation or stealing and necessitates the event of methodologies that ensure the privacy of PHRs. Existing hospital system does not contain multi-hospital appointment booking system. Proposed system overcomes certain drawbacks of existing system. The patients search nearest hospitals on the application and get no of nearest hospitals with their ratings reviews and waiting time. Patients send appointment requests to hospital and get confirmation of the hospital through the message. Multiple doctors can share the same patients for treatment.

**Keywords—** Book appointment, feedback, Encryption, nearest location.

## I. INTRODUCTION:

Cloud computing is widely utilized by people and organizations (including government agencies), to store and access massive volume of knowledge (e.g., text, image, and video), that is not generally encrypted before outsourcing. Searchable encoding (SE) schemes alter user's knowledge to firmly search and through selection retrieves records of interest over encrypted knowledge (outsourced to the cloud), in line with user-specified keywords. However, there are different fascinating properties once coped with encrypted knowledge outsourced to the cloud. For instance, once encrypting an important volume of knowledge, typical encoding approaches end up with limitations due to multiple copies of ciphertexts (e.g., publically key encoding schemes) and complicated, big-ticket key management (e.g., in radial encoding schemes).

Ciphertext-Policy Attribute-Based encoding (CP-ABE) schemes are designed to mitigate these two limitations, also enhancement of access permissions in multi-user settings and facilitating one-to-many encoding.

## II. LITERATURE REVIEW:

*Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting (2019)[1]*

This paper incorporates Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) which facilitates query search and it assists fine grained access control over the encoded data on cloud. This is a privacy preserving system with hidden access policy in shared multi-owner setting. Furthermore, it shows how the system is improvised to support malice user tracking. The proposed ABKS system also attains discerning security. We assess the system's performance using real-world datasets.

*Student Residential Distance Calculation using Haversine Formulation and Visualization through Google Maps for Analysis[2]*

In this paper, data mining concept is used. In the proposed system, they are using Haversine algorithm for calculating distance between two addresses. Google Maps API is also used to calculate longitude and Latitude of each and every address. Using this concept they will calculate the distance of two points on the GPS. Haversine Algorithm helps in finding great-circle distance between two points on a sphere given their longitudes and latitudes. In this paper GMap is basically used for direction and transit, traffic conditions, street view.

*SeSPHR : A Methodology for Secure Sharing of Personal Health Records in the Cloud[3]*

In this paper, a methodology called the SeSPHR is proposed for sharing the PHR's securely on cloud. This scheme allows to preserve the confidentiality of the health records and grants access to users. SeSPHR provides security against insider threats. It also enforces back and forth access control. This project ensures patient-centric control on the PHRs as well. Patients store all of their health records on the untrusted cloud servers and selectively grants access to diverse users on various portions of the health records.

*Reduced outpatient waiting times with improved appointment scheduling: a simulation modeling approach[4]*

When we have an emergency condition, we often have to deal with unknown variables such as travel, distance and time of the medical services near us. In this paper, the author has concentrated on the effects of travel time and waiting time and especially on the waiting time elasticity of demand. An effective appointment system is a critical

component in controlling patient waiting times within clinic sessions. Current waiting times are often unacceptable and cause great stress on clinic staff. This paper describes the development and use of a detailed simulation model of an Ear, Nose and Throat (ENT) outpatient department. Basically this model will help to reduce waiting time of the patient.

*MD5 research[5]*

MD5 is also known as Message Digest Algorithm 5 is the fifth generation on behalf of the message digest algorithm. The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message. In August 1992, Ronald L. Rivest submitted a document to the IETF entitled "The MD5 Message-Digest Algorithm", which describes the theory of this algorithm. This algorithm is basically used for data security and data integrity. MD1, MD2, MD3, MD4 developed MD5. It can compress any length of data into an information digest of 128bits. It is used as a secure cryptographic hash algorithm for authenticating digital signatures.

III. RELATED WORK:

In the existing system, patient's appointments are booked manually and waiting time is not known earlier. Sometimes patients are in a new place and are in an urgent need of a good hospital, but they fail to get one because of lack of communication. One serious limitation of CP-ABE schemes is that the access policy embedded in the ciphertexts may leak sensitive information to authorized data users, as discussed in the preceding section .

Disadvantages:

- Manually book the appointments.
- Waiting time not confirmed for new patients.

IV. PROBLEM STATEMENT:

Nowadays, storing the records on cloud is very complicated and insecure for the users. Users spend most of their time in the hospitals because they don't know how long to wait for consultation. Also, patients have no idea about how effective the services provided by the hospital are. To overcome this issue we want to develop an application that permits book appointments in the required hospital that is closer to the user by considering the reviews on the hospitals. Users can view all the nearest registered hospitals with distance and direction, users can also get the details about the waiting time.

V. PROPOSED SYSTEM

Our aim is to present hospitals with a centralized system which will digitally monitor and manage records of multiple hospitals at once. Patients should digitally book his/her appointment to the nearby hospital he/she wants to admit. This will help patients to save his/her waiting time in the hospital. Also he/she will get non erasable secure records via cloud. Patient's data can have multiple

owners(patient's data can be accessed by multiple doctors) depending upon patient's needs(disease type). Our main objective is to implement multiple owner settings so that patient data can be shared among multiple doctors of the same hospital for recovery.

In our system, we are using time servers (for waiting time of the patients), ranking and reviews (for Feedback regarding hospitals services) and Google Maps API (Locating nearest hospitals from patient's location). Proposed System has the following actors:

**Admin:**

- Add and remove Hospitals with longitude and latitude.
- Add and Remove the main Doctor and assign rights to them.
- View Hospitals details.

**Main Doctor:**

- Add and Remove Doctors and members.
- View Patient details.

**Doctors:**

- Checks for Patients' appointment requests.
- Attend Patients, prepare Prescription and fix fees based on disease.

**Receptionist:**

- View Patients appointment requests and assigns doctors who are free accordingly.
- Send confirmation messages to respective patients.
- Manage billing details of patients.

**Patients (Users):**

- Can search for Hospitals nearest to them(Using haversine algorithm and GMaps API).
- Can view Hospitals along with waiting time(Time Server).
- Can request for booking an appointment.
- Can provide feedback of Service in terms of Review and ratings.

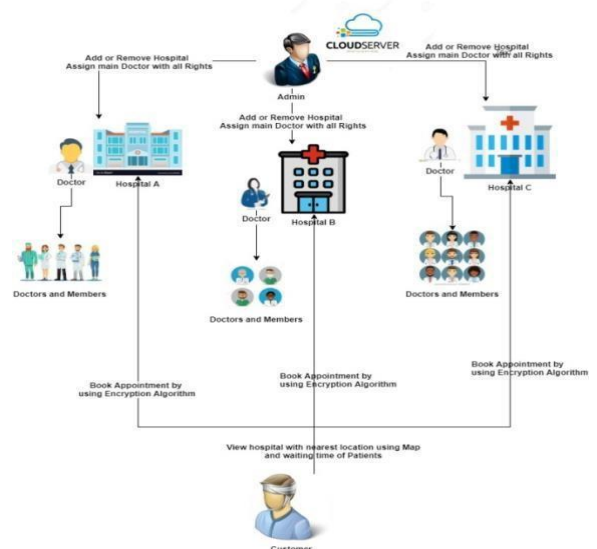


Figure 1 System Architecture

#### CONCLUSION:

Implementation of the 'Efficiently Sharing Personal Health Records between Users and Doctors on cloud' project helps to store all kinds of secured records, provide user communication and coordination, implement policies, improve day-to-day operations, arrange the supply chain, manage human and financial resources, and market hospital services digitally.

Along with this, System automatically encrypts those details and sends them to the hospitals. System has covered non existing features like saving the waiting time of patients, directing them to effective services provider hospitals using ratings and reviews. Booking of nearby hospitals on fingertips, Non erasable records of appointment with prescriptions, notifying patients for their appointments, personalized search results of hospitals based on patient disorder, etc.

In our system, the admin adds hospitals and main doctors and gets daily updates. Admin sets rights to the doctor and makes the main doctor add or remove any members or doctors of that particular hospital. Users search for hospitals and the system displays hospital names with waiting time that are nearest to a user. The user books an appointment and enters his personal details.

#### REFERENCES

- [1] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785–796, 2017.
- [2] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Transactions on Services Computing*, vol. PP, pp. 1–1, 2018.
- [3] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2017.
- [4] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privacy (SP 2000)*, 2000, pp. 44–55.
- [5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. International conference on the theory and applications of cryptographic techniques (EUROCRYPT 2004)*, 2004, pp. 506–522.
- [6] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 312– 325, 2016.
- [7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symposium on Security and Privacy (SP 2007)*, 2007, pp. 321–334.