SECURE DATA SHARING IN CLOUD COMPUTING FOR PERSONAL HEALTH CARE INFORMATION

NARASIMHAREDDY VENNA, M.Tech
Department of Computer Science,
Vidya Jyothi Institute of Technology, Hyderabad.

A. SWARNA
Assistant professor
Dept of CSE., Vidya Jyothi Institute of Technology, Hyderabad.

RAVI MATHEY
Professor,
Dept of CSE. Vidya Jyothi Institute of Technology, Hyderabad.

ABSTRACT

Personal Health Record has emerged as a patient-centric model of health info exchange. A private Health Record service permits a patient to make, manage, and management her personal health information in one place through the net, that has created the storage, retrieval, and sharing of the medical info additional economical. Especially, every patient is secure the complete management of her medical records and might have her health information with a good vary of users, together with tending suppliers, members of the family or friends. Intensive analytical and experimental results area unit bestowed that show the protection, quantifiability and potency of our planned theme.

Keywords: - Personal health records, cloud computing, data privacy, Management, virtual machine, verification

INTRODUCTION

A Personal Health Record service permits a patient to make, manage, and management her personal health knowledge in one place through the online, that has created the storage, retrieval, and sharing of the medical info additional economical. Especially, every patient is secure the total management of her medical records and might have her health knowledge with a large vary of users, together with aid suppliers, members of the family or friends.

As a result of the high value of building and maintaining specialised knowledge centres, several Personal Health Record services area unit outsourced to or provided by third-party service suppliers, for instance, Microsoft HealthVault1. Recently, architectures of storing Personal Health Record in cloud computing are projected in. whereas it's exciting to own convenient Personal Health Record services for everybody, there area unit several security and privacy risks the worth of home-based health watching has been recognized late
Studies 24-hour mobile watching System that Perform home-based health watching tasks. During this paper, we have a tendency to endeavour to review the patient-centric, secure sharing of PHRs keep on semi trusty servers, and target addressing the difficult and difficult key management problems. so as to safeguard the non-public health knowledge keep on a semi trusty server, we have a tendency to adopt attribute primarily based secret writing (ABE) because the main secret writing primitive.

Using ABE, access policies area unit expressed supported the attributes of users or knowledge, that permits a patient to by selection share her PHR among a group of users by encrypting the file beneath a group of attributes, while not the requirement to understand a whole list of users. The complexities per secret writing, key generation, and decipherment area unit solely linear with the amount of attributes concerned. However, to integrate ABE into an outsized scale PHR system, necessary problems like key management quantifiability, dynamic policy updates, and economical on-demand revocation area unit nontrivial to resolve, and stay mostly open up-to-date.

**Existing system**

We tend to contemplate a private Health Record system wherever there area unit multiple Personal Health Record house owners and private Health Record users. The house owners consult with patients United Nations agency have full management over their own Personal Health Record knowledge, i.e., they will produce, manage and delete it. there's a central server happiness to the non-public Health Record service supplier that stores all the owners’ Personal Health Record. The users could come back from numerous aspects; for instance, a friend, a caregiver or a man of science.

Users access the non-public Health Record documents through the server so as to scan or write to someone’s PERSONAL HEALTH RECORD, and a user will at the same time have access to multiple owners’ knowledge. A typical Personal Health Record system uses customary knowledge formats. For example, continuity-of-care (CCR) (based on XML knowledge structure), that is wide utilized in representative PERSONAL HEALTH RECORD systems together with Indio, associate ASCII text file Personal Health Record system adopted by Boston Children’s Hospital. as a result of the character of XML, the non-public Health Record files area unit logically organized by their classes in a very gradable method.

**DISADVANTAGES**

- Difficult for long medication
- Several styles of medication identification
- Frustration of missing doses
- Manual Insurance rise

**PROPOSED SYSTEM**

To assure the patients’ management over their own Personal Health Record, it's a promising technique to write the non-public Health Record before outsourcing. Yet,
problems like risks of privacy exposure, quantifiability in key management, versatile access and economical user revocation, have remained the foremost necessary challenges toward achieving fine-grained, cryptographically enforced knowledge access management.

During this paper, we tend to propose a unique patient central framework and a set of mechanisms for knowledge access management to non-public Health Record hold on in semi-trusted servers. to attain fine-grained and scalable knowledge access management for private Health Record, we tend to leverage attribute primarily based encoding (ABE) techniques to write every patient’s Personal Health Record file. Totally different from previous works in secure knowledge outsourcing, we tend to specialize in the multiple knowledge owner state of affairs, and divide the users within the Personal Health Record system into multiple security domains that greatly reduces the key management complexity for house owners and users.

A high degree of patient privacy is secure at the same time by exploiting multi-authority ABE. Our theme additionally allows dynamic modification of access policies or file attributes supports economical on-demand user/attribute revocation and break-glass access underneath emergency situations.

**ADVANTAGES**
Extensive analytical and experimental results area unit conferred that shows

- Scalability
- Security
- Efficiency.

**SYSTEM ARCHITECTURE**

**Modules Description**

**Admin Process:**

In admin process of our project as, Patient details registration, Hospital details registration. Insurance company registration and emergency hospital registration. Those details are stored in cloud space.
Patient Interactions:

The main goal of this project is to maintain patient records and reports and using this in worldwide. In our project patient’s interaction is must. Each and every patient having a patient id and password. When will the patient entering our health website, they will view their health report and current status.

Hospital Maintenance:

Every hospital details, licence information’s are maintained by Personal health record owner. Those details are maintained and stored to cloud database in encrypted format.

License & Passport Verification:

Every hospital and doctors having their own licence. Our PHR owner verifies that licence details and passport verification for getting a authorized doctor. If the license will be in expired, the PHR owner notifies that particular hospital or doctor for license renewal.

Insurance Process:

In this module provides the insurance to patients. First it checks some particular details about patient for verification. That is, whether the patient got a treatment or not. After verification, the insurance will provide to patients.

Attribute Encryptions:

In our project each and every details saves to database in encrypted form. Like patients details, hospital details, licence details, insurance details etc., those details are encrypted by using some of algorithms. Such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), Triple DES and MD5 (Message-Digest).

Emergency Process:

Due to any emergency process, it contains some emergency hospital details. So any one emergency mean, it’s directly communicated to emergency hospital for their treatments.

AES (Advanced Encryption Standard):

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware.

CONCLUSION

In this paper, we’ve projected a completely unique framework of secure sharing of private health records in cloud computing. Considering partly trustworthy cloud servers, we tend to argue that to completely understand the patient-centric thought, patients shall have complete management of their own privacy through encrypting their PHR files to permit fine-grained access. The framework addresses the distinctive challenges brought by multiple PHR house owners and users, in this we tend to greatly scale back the quality of key management whereas enhance the privacy guarantees compared with previous works. We tend to
utilize ABE to inscribe the PHR knowledge, in order that patients will permit access not solely by personal users, however additionally numerous users from public domains with totally different skilled roles, qualifications and affiliations. What is more, we tend to enhance associate degree existing MA-ABE theme to handle economical and on-demand user revocation, and prove its security.

REFERENCES
