PRIVACY PRESERVATION OF E-HEALTH CARE SYSTEM IN CLOUD

Sayali Ravindra Balapure¹ and Prof. Priti Khodke²
¹²Computer Sciences and Engineering, PRMCEAM, Badnera, Amravati, India

Abstract- E-health care system is one way for patients to storing their personal health data online with privacy. There are various approaches used for e-health care system like Holistic approach, Wireless sensor network based approach, Agent based approach, Architectural approach, 2G RFID based and Cloud computing based approach etc. This number generator for unlinkability. In this system using a secure indexing method for privacy preserving keyword search, which hides both search and access patterns based on redundancy. And integrate the concept of attribute based encryption with paper focus on the cloud computing based approaches for e-health care system. For this purpose different cloud based system with various pseudorandom key generation. There are also using the open source platform for cloud. Recommender system especially using for retrieval at emergencies and making inspection for misusing health data. Specifically, we propose to integrate key management from pseudorandom auditability to prevent potential misbehavior, in both normal and emergency cases.

Keywords- e-health system, privacy, security, cloud computing, personal health record.

I. INTRODUCTION

Electronic health care system provides services provisioning, helps saving life by providing timely treatment to patients in medical emergencies. Electronic healthcare system is anytime and anywhere accessible plays an important role in our daily life. These services are supported to mobile devices such as home care and remote monitoring by users. Researched works are concluded early and specialized pre-medical treatment contributes to survive the emergency case and fast response to emergency case.[2] That is given the results about out coming improvement of patient’s health.

Related reference paper address the emergency response problem from “mobile healthcare social network (MHSN)” perspective: Enabling a patient to locally search for the nearby physicians via a self-organized manner. In MHSN, some users are patients equipped with wireless body sensors that can be used to monitor body physiological condition, and they need medical services in the emergency situation. Some physicians or paramedics are capable of providing medical services to patients who are in need of emergency care. Mobile healthcare social networks are serving as a mobile community platform for healthcare purposes. They extend the traditional centralized healthcare system by placing great emphasis on user self-organized and social interactivities. An essential capability offered by MHSN is to allow mobile patients to search, recognize, and interact with physicians who locate in their physical vicinity. In MHSN each user has equipped with personal digital assistant (PDA) and able to connect wirelessly to a one-hop neighboring user without the involvement of any third party. In MHSN, some users are patients equipped with wireless body sensors that can be used to monitor body physiological condition, and they need medical services in the emergency situation. Some physicians or paramedics are capable of providing medical services to patients who are in need of emergency care.

Some other related reference paper are concluded that these e-healthcare systems are increasingly popular and a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace. There are good reasons for keeping medical data private and limiting the access.[5] Personal Health Record (PHR) service is an emerging model for health information
exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. Advance technology of cloud computing PHR has undergone substantial changes. Most health care providers and different vendors related to healthcare information technology started their PHR services as a simple storage service.[1] After turn those into complicated social networks like service for patient to sharing health information to others with the emergence of cloud computing. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client’s data, a novel patient centric framework is used.[1] They introduce the private cloud which can be considered as a service offered to mobile users.

II. PERSONAL HEALTH RECORD SYSTEM

Fast access to health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted. While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace.[2] Electronic Health Record (EHR) has a lot of definitions, such as the electronic record that keeps patient’s medical information in a health record system managed by healthcare providers. Despite EHR positive impact on healthcare services; its adoption progress is slow in most healthcare institutions worldwide; especially in developing countries due to several common challenges. Security of patient data has been a concern from the beginning of medical history and is still a key issue in contemporary age. The Oath of Hippocrates was instituted on the principle of confidentiality, and has thus turned out to be an honored action in clinical and medical ethics. Protecting the privacy and confidentiality of patient information is of utmost importance; security gives rise to trust. Security of medical records mainly covers confidentiality and privacy. Cloud computing introduces the possibility to access large volumes of patient information in a short period. This increases the chance of an unauthorized person accessing patient records easily.[4] The management of private and confidential information is a major problem for dynamic organizations. Secure solutions are needed to exchange confidential documents, protect them against unauthorized accesses and cope with changes of people’s roles and permissions. Traditional cryptographic systems and PKI show their limitations, in terms of flexibility and Manageability. The related paper describes an innovative technical solution in the area of secure messaging that exploits Identifier based Encryption (IBE) technology. It illustrates the advantages against a similar approach based on traditional cryptography and PKI. It discusses a few open issues. The main contribution is a practical solutions based on IBE technology. A secure messaging system based on IBE has been fully implemented and it is used in a trial with a UK health service organization.[6]

III. E-HEALTH CARE SYSTEM WITH CLOUD COMPUTING

With the help of cloud computing, personal health record are worked more efficiently. The personal health records are worked with open source cloud platform. These access the data from cloud with robust and secured while outsourcing data. To maintain the privacy preserving while data access in cloud with the help of various encryption techniques. There are various encryption
techniques as well as privacy preserving mechanism for data access. A secure EHR system to protect patient privacy and enable emergency healthcare. The system is demonstrated to be resilient to various attacks, fulfill the desired functionalities, satisfy the security requirements, and maintain a good balance between security and efficiency. [8] Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this referred paper they begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. They consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. They formally define SSE in this multi-user setting, and present an efficient construction. [7]

E-Health systems have replaced paper based medical system due to its prominent features of convenience and accuracy. Also, since the medical data can be stored on any kind of digital devices, people can easily obtain medical services at any time and any place. However, privacy concern over patient medical data draws an increasing attention. In the current e-Health networks, patients are assigned multiple attributes which directly reflect their symptoms, undergoing treatments, etc. Those life-threatened attributes need to be verified by authorized medical facilities, such as hospitals and clinics. [10] When there is a need for medical services, patients have to be authenticated by showing their identities and the corresponding attributes in order to take appropriate healthcare actions. However, directly disclosing those attributes for verification may expose real identities. Therefore, existing e-Health systems fail to preserve patients' private attribute information while maintaining original functionalities of medical services. To solve this dilemma, we propose a framework called PAAS which leverages users' verifiable attributes to authenticate users in e-Health systems while preserving their privacy issues. In this system, instead of letting centralized infrastructures take care of authentication, our scheme only involves two end users. We also offer authentication strategies with progressive privacy requirements among patients or between patients and physicians. [9] Following figure shows the general architecture of e-health care system.

![Figure 1: General architecture of e-health system.](image)

**IV. ANALYSIS OF E-HEALTH SYSTEM**

In this section we describe the all comparative analysis of all different methodology can used by personal health record. In these review paper, we referred the various reference papers about personal health record. There are various techniques are used for providing security to the personal health data. Various encryption techniques, [17] privacy mechanism, random key generation, wireless body sensor etc are used [19]. This review paper is analysis with all factor of e-health system like
time complexity of e-health system, take a review of key size and block size are used by encryption algorithms, how various security algorithms are used by e-health care system. The cloud computing are used for storing the user's personal health information and sharing and accessing the information with privacy preserving mechanism.[20] The referred paper are summarized the various privacy preserving mechanism related with cloud computing. There are some issues related with security and privacy of e-health system. This paper focus on provides security to the patients personal health record. This paper analysis the all security constraints of e-health system. In this paper, analysis all features of various method of cloud based e-health care system. There are various encryption techniques are also used for building the e-health system based on cloud computing.[14] There is a comparison table of various cloud computing system based on e-health system. This table shows the various methodology of various system used by e-health system.

<table>
<thead>
<tr>
<th>Sr.no</th>
<th>Methodology is used</th>
<th>Purpose of system</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Secure indexing and attribute based encryption</td>
<td>To integrate key management from pseudorandom number generator for unlink ability.</td>
<td>Efficient key management. Privacy preserving data storage. Retrieval especially for retrieval at emergencies. Audibility for misusing health data.</td>
</tr>
<tr>
<td>2</td>
<td>Attribute based broadcast encryption with fine grained control access</td>
<td>To a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained scalable access for PHRs.</td>
<td>It uses on demand revocation. It is flexible. Break glass access for emergency.</td>
</tr>
<tr>
<td>3</td>
<td>It supports efficient on demand revocation with CP-ABE</td>
<td>To propose novel patient-centric framework and suite of mechanism for data access control to PHRs stored in semi trusted servers.</td>
<td>To maintain data security. To centralize the user’s personal information.</td>
</tr>
<tr>
<td>4</td>
<td>Wireless Body sensor network</td>
<td>This paper proposed to satisfy other fundamental security goals besides the privacy requirements.</td>
<td>This scheme satisfied authentication, privacy, confidentiality, integrity of system.</td>
</tr>
<tr>
<td>5</td>
<td>RDM200 Delegation</td>
<td>To propose a rule-based framework for role-based delegation.</td>
<td>Focus on user to user delegation. There are users delegating her role to another user.</td>
</tr>
<tr>
<td>6</td>
<td>HCCPP: Cryptography based system</td>
<td>This paper a propose a secure EHR system, HCCP (Healthcare system for Patient Privacy), based on cryptographic constructions.</td>
<td>This system satisfied all security requirements of system.</td>
</tr>
<tr>
<td>7</td>
<td>Ad hoc network</td>
<td>This paper proposes reducing location resolution for safety protection, and present distributed cloaking algorithms for both stationary and mobile ad hoc networks.</td>
<td>It done the protection from location cloaking.</td>
</tr>
<tr>
<td>8</td>
<td>Gap Diffie-Hellman (GDH) group signature schemes</td>
<td>It proposed a robust proactive threshold signature scheme, a multi signature scheme and a blind signature scheme.</td>
<td>It is more efficient.</td>
</tr>
<tr>
<td>9</td>
<td>Searchable symmetric encryption</td>
<td>The objective of this paper is to introduce a review of the three schemes with a discussion in the advantages and disadvantages of each.</td>
<td>It deals with larger data file.</td>
</tr>
</tbody>
</table>

Table 1: Comparison of various methods used by e-health system.
V. CONCLUSION AND FUTURE WORK

In this paper, the review of different cloud computing based e-health care system is presented. The features of all these systems are compared in Table 1. It includes all encryption techniques which help to preserve the privacy for personal health record. The cloud based system makes personal health record more efficient and flexible. With the help of cloud based system we can say that it help the user to save time and efforts during the health system. In the e-health care system, encryption technique is allowing the outsourcing data with security.

In the future work, although the tool is prepared for supported to stored and shared transaction, and it is provided to users, it has some limitation. The popularity of cloud computing is increased day by day, due to these there is chances increase lost of data and storage problem faced by user. Although these parameter tradeoff with complexity and performance. There are increasing cost factor also faced by user. The robustness and estimation of performance boundary are currently under investigation. In this system multiple user with multiple data centers are also done in future.

REFERENCES

[16] Toby Xu, Ying Cai; Location Cloaking for Safety Protection of Ad Hoc Networks.

[23] Ning Cao, Zhenyu Yang, Cong Wang, Kui Ren, and Wenjing Lou; Privacy-Preserving Query over Encrypted Graph-Structured Data in Cloud Computing.